D. Access Rights under the Interoperable Eurodac

I. The Right to Information

1. What Is the Right to Information?

The right to information is contained in all regulations regarding large-scale databases in the Schengen Area, including the Eurodac Regulation[513] and the Interoperability Regulations,[514] as well as in the GDPR,[515] the Police Directive,[516] and the Data Protection Directive for EU Institutions and Bodies.[517]

The right to information, as it is understood in this study, is the right to be informed about the use of one's data, without having to submit an access to information request. This is different from the right to information contained in Art. 10 and 11 TEU or Art. 15 TFEU. These provide a right that institutional decision-making has to be carried out "as closely as possible to the citizen"[518] and that EU institutions are obliged to act publicly and to ensure that individuals and any natural or legal person residing or having its registered office in an EU country can access documents.[519] In this study, the right to information describes the right to receive information on the use of one's personal data, during the process of providing such data to a Member State. The right to be informed in that sense forms part of the principle of transparency in data protection law.[520] This principle is

513 2016 Eurodac Proposal, Art 30.

514 Interoperability Regulation - Judicial Cooperation, Art 48; Interoperability Regulation - Borders, Art 48.

515 GDPR, Art 12.

516 Police Directive, Art 13.

517 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) [2018] OJ L295/39 (Data Protection Regulation for EU Institutions and Bodies), Art 15.

518 TEU, Art 10.

519 TFEU, Art 15.

520 GDPR, Art 5 states that personal data shall be processed "lawfully, fairly and in a transparent manner in relation to the data subject"; GDPR, Art 12 mandates con-

safeguarded explicitly in primary law by Art. 8(2) sentence 2 CFR, in the way that this provision grants every person the right to obtain information about the data collected concerning them.[521] It can, however, also be derived from other human rights provisions, like Art. 8 ECHR. The goal is thus to ensure that data subjects understand the purpose for which their data are collected and processed, by whom it is processed, and who can access it. It is a precondition to effectively exercise the right to access, correction, and deletion of personal data.[522]

The peculiarity, or rather the challenge, in connection with Eurodac is that the data subjects are applicants for international protection and persons apprehended in an irregular situation, some of them minors, persons with disabilities or trauma. Providing them with all the information legally required is not an easy undertaking, as this chapter will show. The Interoperability Regulations add additional challenges to the task.

a) *International Human Rights Law Applicable in Europe*

The right to information in the Eurodac and Interoperability Regulations cannot be assigned to a single fundamental right in the ECHR. The right, in the context of the EU information systems, is based on the principle of transparency and fairness of data processing, which has been developed under Art. 8 ECHR[523] and Art. 10 ECHR.[524] In several cases concerning

---

trollers to take appropriate measures to provide information related "to processing to the data subject in a concise, transparent, intelligible and easily accessible form".

521 Alexander Roßnagel, 'Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten' in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019), para 49.

522 Case C-203/15 *Tele2 Sverige* [2016] OJ C 53/11, para 121; Alexander Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection Regulation: Article-by-Article Commentary* (1st edn, Bloomsbury Publishing 2023), para 7; Matthias Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020), para 8; GDPR, Art 13; Interoperability Regulation - Borders, Art 13.

523 E.g., *Torsten Leander v Sweden* [1987] ECtHR Series A no 116; cf ECHR, 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (2023).

524 E.g., *Gaskin v the United Kingdom* [1989] Series A no 160; *Torsten Leander v Sweden* (n 523).

personal data collected and stored by public authorities, the ECtHR found that the authorities had a positive obligation to provide those concerned with an "effective and accessible procedure" to allow them to have access to "all relevant and appropriate information" necessary to understand their data and how it has been processed; and in this context, it recognised a right to information.[525] The right to information is also part of the right to access (or receive) information held by public authorities which generally falls within the ambit of Art. 10 ECHR,[526] but can be based on the right to life, Art. 2 ECHR, and the right to a fair trial as well as equality of arms in Art. 6(1) ECHR.[527]

The rights to privacy and freedom of expression are furthermore contained in other international human rights instruments, like Art. 12 and 19 UDHR, which is not a binding instrument. Art. 17 and Art. 19 ICCPR hold binding rights to privacy and to freedom of expression. There are provisions for certain categories of persons. Art. 21 CRPD states that State Parties must ensure that all persons with disabilities can enjoy the "freedom

525 *Gaskin v the United Kingdom* (n 524), para 49; *Odievre v France* [2003] ECHR 86, para 41-49; *Roche v the United Kingdom* [2005] ECHR 2005-X, para 162; *Guerra and Others v Italy* [1998] EHCR 7, para 60; *McGinley and Egan v the United Kingdom* [1998] ECHR 51, para 101.

526 Council of Europe, 'The Right of Access to Information, A Key Prerequisite for the Freedom of Expression' (2018) 1; There is not (yet) a general right to obtain information from public authorities and access official documents (Päivi Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (2013) 5 Journal of Media Law 79, 102; David Banisar, 'Freedom of Information Around the World 2006: A Global Survey of Access to Government Information Laws' [2010] SSRN Electronic Journal 168). The Council of Europe and the ECHR generally do not impose on Member States positive obligations to collect and disseminate information of its own motion (cf Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (above n 526)). The ECtHR has, however, considered that in certain circumstances, ECHR, Art 10, can impose such obligations (A positive obligation to guarantee the right to receive information was for example demonstrated in the case *Khurshid Mustafa and Tarzibachi v Sweden* [2008] ECHR 1710. In *Sdružení Jihočeské Matky v Czech Republic* App no 19101/03 (ECtHR, 10 July 2006), the Court pronounced that the refusal of the Czech authorities to supply information was to be considered an interference with the right to receive information as guaranteed by ECHR, Art 10. However, the Court has traditionally been reluctant to derive from ECHR, Art 10 a general right of access to public or administrative documents e.g., *Gaskin v the United Kingdom* (n 524); *Torsten Leander v Sweden* (n 523), para 74; *Stephen Eccleston v the United Kingdom* App no 42841/02 (ECtHR, 18 May 2004), para 3.

527 cf Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (n 526).

to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice". The CRPD includes, in Art. 25, the respect for the elderly to lead a life in dignity and independence. With regard to children, the Convention on the Rights of the Child (CRC)[528] can be read in conjunction with Art. 24 CFR to provide a right to information. Pursuant to Art. 24 CFR, the right to information is a precondition for the child to exercise their right to be heard in judicial and administrative proceedings affecting them, which is protected by Art. 12 CRC and Art. 24 CFR. The CRC Committee states that refugee and migrant children must be "fully informed throughout the entire procedure, together with their guardian and legal adviser, including information on their rights and all relevant information that could affect them".[529] Refugee and migrant children should receive all necessary and relevant information, as early as possible.[530] A determination of when a child is capable, for example, of consenting to the processing of their personal data, has to consider their actual understanding of the data processing along with their best interests, rights, and views.[531]

Finally, the Council of Europe Convention 108, which opened for signature on January 28, 1981, was the first legally binding international instrument in the field of data protection, aimed at safeguarding individuals with respect to the processing of their personal data.[532] It was signed by 46 Members of the Council of Europe and nine non-Members.[533] The modernised version, Modernised Convention 108+, was adopted in 2018. The Convention does not grant a right to information as such; rather, it stipulates

528 Convention on the Rights of the Child [1989] (CRC).

529 UN Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families (CMW), 'Joint General Comment No. 4 (2017) of the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families and No. 23 (2017) of the Committee on the Rights of the Child on State Obligations Regarding the Human Rights of Children in the Context of International Migration in Countries of Origin, Transit, Destination and Return' (2017) CMW/C/GC/4-CRC/C/GC/23, para 17.

530 UN Committee on the Rights of the Child (CRC), 'General Comment No. 12: The Right of the Child to Be Heard' (2009) CRC/C/GC/12, para 134(a).

531 Joseph Cannataci, 'Special Rapporteur on the Right to Privacy' (UN Human Rights Special Procedures 2020).

532 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981] No. 108 (Convention 108).

533 'Chart of Signatures and Ratifications of Treaty 108' (*Council of Europe Portal - Treaty Office*, 1 August 2024) <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

that each Party must ensure, within its legal framework, that all rights it provides – such as the rights to access and rectification – are available to every data subject. Additionally, parties must offer the necessary legal and practical means to exercise these rights effectively and adequately.[534] The right to information is understood as a precondition for exercising said rights.

b) *EU Human Rights Law: European Charter of Fundamental Rights*

aa) Rights to Privacy

The European Charter of Fundamental Rights contains two rights regarding privacy. Art. 7 CFR states that "[e]veryone has the right to respect for his or her private and family life, home and communications". Art. 8(1) CFR contains the right to protection of personal data. According to paragraph 2, data must be processed "fairly for specified purposes on the basis of the consent of the person or another legitimate basis laid down by law". It further contains the right of every person to access and rectify data concerning them. Art. 8(2) sentence 2 CFR is understood to explicitly safeguard the principles of transparency in primary law, in the way that this provision grants every person the right to obtain information about the data collected concerning them.[535] The transparency requirement – like all data protection law – is related to the protection of the (external) rights and freedoms of the data subject in general.[536] Paragraph 3 stipulates that the control of compliance with these rules shall be carried out by an independent authority.

Art. 7 and 8 CFR are closely linked. The CFR is unique, as an international human rights instrument, in recognising the right to data protection

534 Modernised Convention 108+, Convention for the Protection of Individuals with Regard to the Processing of Personal Data [2018] (Modernised Convention 108+), para 71.

535 Roßnagel, 'Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten' (n 521), para 49.

536 Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 8.

as a right separate from the right to privacy.[537] For instance, the right to data protection as such cannot be found in the ECHR.

The Court of Justice of the European Union (CJEU) does not apply a consistent approach to the distinction between Art. 7 and Art. 8 CFR.[538] Often, the two rights are assimilated and an assessment is made whether the infringement can be justified under Art. 52(1) CFR.[539] According to Kullman, the interconnection between Art. 7 and 8 CFR will likely continue as the CJEU and other institutions, such as the EDPS, consider these rights together.[540]

The overlap of these two rights stems from the common origin of the two articles in Art. 8 ECHR and its case law.[541] While Art. 7 CFR is primarily rooted in Art. 8 ECHR, Art. 8 CFR has several sources; it is especially influenced by the Council of Europe Convention 108.[542,543] The ECJ even

537 Herke Kranenborg, 'Article 8 – Protection of Personal Data' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Bloomsbury Publishing 2021), para. 8.30.

538 ibid, no. 8.46; Tobias Lock, 'Charter of Fundamental Rights of the European Union - Article 7 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (1st edn, Oxford University Press 2019), para 6.

539 Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), no. 8.46.

540 Miriam Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life', *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Peer/Harvey/Kenner/Wald 2022) no 7.73; similar: Tobias Lock, 'Charter of Fundamental Rights of the European Union - Article 8 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (1st edn, Oxford University Press 2019), para 3; EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 7 - Respect for Private and Family Life.

541 Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), no. 8.30; Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life' (n 540), no 7.78A; Lock, 'Article 7 CFR' (n 538), para 1 and Lock, 'Article 8 CFR' (n 540), para 1; EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79) Article 7 - Respect for Private and Family Life; The point remains pertinent as it has been referred to in decisions including, for example, AG Paolo Mengozzi, 'Opinion 1/15 on the Draft Canada-EU PNR Agreement' (Grand Chamber of the Court of Justice of the European Union 2017), para 171.

542 cf Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange At EU-Level* (Springer 2012) 92ff.

543 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 7 - Respect for Private and Family Life; Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life' (n 540), no 7.78; Kranenborg, 'Article 8

stated that Art. 8 CFR concerns a fundamental right that is distinct from that enshrined in Art. 7 CFR and has no counterpart in the ECHR.[544]

In trying to divide the two articles, some scholars state that Art. 7 CFR constitutes a broad statement regarding the respect for private life. Conversely, Art. 8 CFR provides for protection in processing of personal data. Where these two articles intersect, Art. 7 CFR forms a broader protection of the right to respect for private life, home, and communications, whereas Art. 8 CFR seems to be a particularised subset of privacy focusing upon personal data.[545] It has even been suggested that Art. 8 CFR could be considered *lex specialis*.[546] The ECJ's Opinion 1/15 illustrates this confluence: fingerprints and facial images fall within Art. 7 CFR's wide scope, which concerns "any information relating to an identified or identifiable individual".[547] These same data, though, must be protected and processed fairly, pursuant to Art. 8 CFR.[548]

Art. 8 CFR has a broad field of application encompassing all areas of EU competence.[549] It contains the right to access one's own personal data and in some cases, according to the CJEU, a right to be actively informed: the ECJ stated in its Tele2 Sverige judgment that data subjects must be notified after their data have been accessed by law enforcement authorities.[550] In Opinion 1/15, the ECJ reiterated this consideration, emphasising that notification is essential for ensuring that individuals can be confident their personal data are processed correctly and lawfully. This notification enables them to exercise their right of access, as well as, if necessary, their right

– Protection of Personal Data' (n 537), no 8.49ff; Lock, 'Article 8 CFR' (n 540), para 1.

544 *Tele2 Sverige* (n 522), para 129.

545 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79) Article 7 - Respect for Private and Family Life; Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life' (n 540), no 7.79A.

546 Lock, 'Article 8 CFR' (n 540), para 3.

547 'Opinion 1/15 on the Draft Canada-EU PNR Agreement' (n 541), para 122; Joined Cases C-92/09 and C-93/09 *Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] OJ C 13/6, para 52; *Case C-291/12 Michael Schwarz v Stadt Bochum* [2013] OJ C 367/17, para 26.

548 'Opinion 1/15 on the Draft Canada-EU PNR Agreement' (n 541), para 123; EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79) Article 7 - Respect for Private and Family Life; Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life' (n 540), no 7.79A.

549 Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), no 8.01.

550 *Tele2 Sverige* (n 522), para 121. The case refers to data retained by electronic communications services.

to rectification and to an effective remedy.[551] The Court also sees the right to information as a prerequisite for the lawful collection and processing of data.[552] Dix, among other scholars, concurs that the obligations to provide information under Art. 13 and 14 GDPR are a concretisation of the fundamental right in Art. 8 CFR.[553]

Art. 52 CFR addresses the possible limitations on the exercise of the rights and freedoms of the Charter. Art. 8(2) CFR already contains some sort of limitation by stating that "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Still, Art. 52 CFR is applicable. It follows that the condition in Art. 8(2) CFR, i.e., that data processing must be based on the consent or a legitimate basis laid down by law, may be limited, but only if this is provided for by law and complies with the other conditions of Art. 52(1) CFR.[554] These are the obligations to respect the essence of the rights and freedoms as well as respect the principle of proportionality. Limitations need to be necessary and genuinely meet objectives of general interest recognised by the EU or to protect the rights and freedoms of others.

Art. 7 CFR has no limitation clause in itself. However, the limitations according to Art. 52 CFR apply in accordance with Art. 52(3) CFR. The meaning and scope of this right are the same as those of the corresponding Art. 8 ECHR.[555] Some scholars have also suggested that Art. 8(2) CFR must be interpreted using the proportionality test under Art. 52 CFR.[556]

---

551 'Opinion 1/15 on the Draft Canada-EU PNR Agreement' (n 541), paras 219 - 220; Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), no 8.162.

552 Case C-201/14 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* [2015] OJ C 381/5, para 43.

553 Alexander Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019), para 2; cf also Orla Lynskey, 'Deconstructing Data Protection in the EU Legal Order: The "Added-Value" of a Right to Data Protection in the EU Legal Order', (2014) 63 International and Comparative Law Quarterly 569; European Data Protection Board (EDPB) 'Guidelines 01/2022 on Data Subject Rights - Right of Access (Version 2.1, Adopted on 28 March 2023)'.

554 Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 8.195.

555 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79) Article 7 - Respect for Private and Family Life; Kullman, 'Article 7 (Family Life Aspects) – Right to Respect for Private and Family Life' (n 540), no 7.11B.

556 European Center for Digital Rights, 'Noyb Observations on EDPB Guidelines 01/2022 on Data Subject Rights – Rights of Access (Version for Public Consultation)' (11 March 2022).

bb) Good Administration, Effective Remedy and Fair Trial

The CFR holds the right to good administration in Art. 41. It states that every person has the right to have their affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union. This right includes, according to Art. 41(2) (b) CFR, "[…] the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy […]." The right to good administration reflects a general principle of EU law.[557] Art. 41 CFR is addressed not to the Member States but solely to the institutions, bodies, offices, and agencies of the European Union.[558]

The principle of transparency, from which, as seen above, the right to be informed is derived, is closely related to the right to an effective remedy and a fair trial in Art. 47 CFR. The precondition for being able to exercise an effective legal remedy is the knowledge of how and by whom one's data are being processed.[559]

c) *EU Law: GDPR, Police Directive and Data Protection Directive for EU Institutions and Bodies*

aa) General Data Protection Regulation

The GDPR applies, according to its material scope in Art. 2(1), to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data that are part of a filing system or are intended to form part of a filing system. Fingerprints, facial images, and biographic data are personal data.[560] Eurodac is consid-

557 Case C-604/12 *H. N. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* [2013] OJ C 202/6, para 49.

558 Joined Cases C-141/12 and C-372/12 *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] OJ C 315/2.

559 cf Herwig CH Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Publishing 2021), para 47.188ff and 47.173ff; Case C-300/11 *ZZ v Secretary of State for the Home Department* [2013] OJ C 225/7, para 53 and the case-law cited.

560 "[A]ny information relating to an identified or identifiable natural person" according to GDPR, Art 4(6); cf on the notion of 'personal data' Article 29 - Data Protec-

ered a filing system in that sense.[561] Art. 3 GDPR defines the territorial scope by stating that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller (the person responsible for the data processing)[562] or a processor (the person processing the data on behalf of the controller)[563] in the Union, regardless of whether the processing takes place in the Union or not. Since in the case of Eurodac and processing under the Interoperability Regulation, the controller and the processor are located in the EU (except for associated Schengen/Dublin countries), the GDPR applies as *lex generalis*, where said Regulations do not apply or provide for regulation.[564] The GDPR is, as its name says, a general regulation, while the Eurodac and Interoperability Regulations specify certain aspects with regard to specific data subjects and situations. The Eurodac Regulation specifies that the GDPR applies to the processing of personal data by Member States conducted in its implementation.[565] This also holds true for the Interoperability Regulations.[566] The personal scope of the GDPR, Art. 1(1), encompasses natural persons to whom information relates. This means: the rules of the GDPR are applicable as *lex generalis* to the data in Eurodac or processed under the Interoperability Regulation.

---

tion Working Party (Art. 29 WP), 'Opinion 4/2007 on The Concept of Personal Data' (2007) 01248/07/EN WP 136.

561 [A]ny structured set of personal data which are accessible according to specific criteria" according to GDPR, Art 4(6). Recital 15 of the GDPR makes clear that manual processing in unstructured files should not be covered by the rules. The GDPR applies when the files are structured according to specific criteria. Excluding the purely manual and unstructured processing of personal data reflects the roots of data protection: the introduction of the computer which made it possible to easily structure and search personal data; Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 8.118.

562 Art. 4(7) GDPR.

563 Art. 4(8) GDPR.

564 Same: Niovi Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (2021) 22 German Law Journal 391; For more on the principle of *'lex specialis derogate lex generalis'* in the EU see e.g. Gerard Conway, 'Conflicts of Competence Norms in EU Law and the Legal Reasoning of the ECJ' (2010) 11 German Law Journal 966.

565 Eurodac Regulation 2024, Recital 77; cf also ibid, Recital 13.

566 Interoperability Regulation – Judicial Cooperation, Recital 53; Interoperability Regulation – Borders, Recital 53.

Under Art. 5(1)(a) GDPR, transparency is included as a fundamental principle (in addition to lawfulness and fairness).[567] Transparency is intrinsically linked to the principles of fairness and accountability under the GDPR.[568] From Art. 5(2) GDPR furthermore follows that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.[569] Transparency is part of the right to human dignity.[570]

As Bäcker has put it, the transparency requirement has three general functions from a fundamental rights perspective: firstly, the individual's internal self-determination depends on being able to obtain knowledge of data processing that affects them. Secondly, the data subject needs to be knowledgeable in order to be able to comment on data processing and to effectively exercise their rights. In this respect, the concern to keep data processing sufficiently transparent for the data subject is closely related to the legal protection guarantee of Art. 47 CFR. Thirdly, the transparency requirement – like all data protection law – is related to the protection of the (external) rights and freedoms of the data subject in general.[571] This principle is also explicitly safeguarded in primary law by Art. 8(2) sentence 2 CFR, in the way that this provision grants every person the right to obtain information about the data collected concerning them.[572] Recital 60 of the GDPR holds that the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide

567 In Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31 (Data Protection Directive 95/46/EC), transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).

568 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) 17/EN WP260 rev.01, 5 para 2.

569 ibid.

570 See Dupré, 'Article 1 - Human Dignity' (n 79); The CJEU has confirmed in its case law that the fundamental right to dignity is part of EU law: Case C-377/98 *Kingdom of the Netherlands v European Parliament and Council of the European Union* [2001] ECR I-07079, paras 70 - 77; Dignity is also mentioned in the 2016 Eurodac Proposal, Art 13 (1)(b), which states that Member States must ensure that the data collected fully respect the human dignity of the person.

571 Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 8.

572 Roßnagel, 'Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten' (n 521), para 49.

the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.

The GDPR states in Art. 13(1) that the controller must provide the data subject with a list of information at the time when the personal data are obtained. The list of information largely overlaps with the one in the Eurodac Regulation. Information must be provided regarding the identity and contact details of the controller as well as the data protection officer, the purpose of the processing, recipients of the personal data and, where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.[573]

Further information needs to be given, according to Art. 13(2) GDPR, where "necessary to ensure fair and transparent processing". This entails the time period for which data will be stored, the right to access, rectify and erase data, or lodge a complaint with the supervisory authority. Also, data subjects have to be informed about the existence of automated decision-making, including profiling[574] and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
While some scholars argue that information according to Art. 13(2) GDPR has to be always provided,[575] others argue that this is only true for part of

573 In that case, the data subject has to be informed about whether an adequacy decision regarding the data protection standard of the country or organisation in question, has been taken by the Commission in accordance with GDPR, Art 45(3). Where not such decision exists, information has to be provided about the "appropriate or suitable safeguards" according to GDPR, Art 46, taken by the data controller or processor and the means by which to obtain a copy of them or where they have been made available. Only in specific situations (such as important reasons of public interest) can data be transferred in absence of an adequacy decision and appropriate or suitable safeguards, according to GDPR, Art 49.

574 Profiling as referred to in GDPR, Art 22(1) and (4), which is profiling that "[...] produces legal effects concerning him or her or similarly significantly affects him or her [as automated processing]. Additionaly, [d]ecisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in ibid, Article 9(1), unless point (a) or (g) of ibid, Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

575 Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), no. 7; Lukas Feiler, Michaela Weigl and Nikolaus Forgo, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' *The EU General Data Protection Regulation (GDPR): A*

the information under paragraph 2[576] or only where it seems necessary to ensure the fairness and transparency of the processing.[577]

Whenever the controller intends to further process personal data for a purpose other than that for which they were collected, the controller shall, according to Art. 13(3) GDPR, provide the data subject, prior to further processing, with information on the other purpose and with any relevant further information, as referred to in paragraph 2.

Art. 14 GDPR contains similar information obligations as Art. 13 GDPR but refers to personal data that have not been obtained from the data subject. This is the case when, e.g., the criminal record of a person from another country is being sought. It is hardly ever the case in relation to data in Eurodac. Art. 12 GDPR contains how information in Art. 13 and Art. 14 GDPR must be provided.[578]

According to Art. 23 GDPR, the rights outlined in Art. 5, 13, and 14 GDPR may be restricted by Union or Member State laws, provided that such restrictions respect the essence of fundamental rights and freedoms. These restrictions must be necessary and proportionate in a democratic society to safeguard a public interest. This includes national or public security, the prevention, investigation, detection, or prosecution of criminal offenses, the execution of criminal penalties, and the protection against threats to public security. Additionally, restrictions may serve other impor-

---

Commentary (2nd edn, Globe Law and Business Ltd 2018), para 106; Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 14 para 23.

576 Rainer Knyrim, 'Artikel 13 - Informationspflicht bei Erhebung von Personenbezogenen Daten bei der betroffenen Person', *Datenschutz-Grundverordnung: DS-GVO* (3rd edn, CH Beck 2024), paras 29 and 40ff.

577 Peter Gola and Dirk Heckmann, *Datenschutz-Grundverordnung VO (EU) 2016/679 Bundesdatenschutzgesetz: DS-GVO / BDSG* (3rd edn, CH Beck 2022), Art 13, para 5, according to which an optional element is included in paragraph 2; Similar is Kai-Uwe Plath, *DSGVO/BDSG/TTDSG* (4th edn, Otto Schmidt 2023), Art 13, para 29 and Recital 60; According to Knyrim, 'Artikel 13 - Informationspflicht bei Erhebung von Personenbezogenen Daten bei der betroffenen Person' (n 576), GDPR, Recital 60 goes in this direction "The controller should provide the data subject with any further information nec-essary to ensure fair and transparent processing taking into account the specific circumstances and con-text in which the personal data are processed."

578 This includes, e.g. contains that the controller must take appropriate measures to provide information on data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. Recitals 38 and 58 also emphasise the need for transparency and special protection for children.

tant objectives of general public interest or aim to protect the rights and freedoms of the data subject or others.

bb) Police Directive

The Police Directive applies, according to Art. 2(1) and Art. 1(1), to the processing of personal data by national law enforcement authorities.[579] The material scope in Art. 2(2) Police Directive corresponds to that of the GDPR. It encompasses data collected under the Eurodac and Interoperability Regulations.

Regarding the right to information, the Police Directive is structured similarly to the GDPR. A list of minimum information that must be provided to the data subjects is contained in Art. 13(1), with additional information provided "in specific cases" in paragraph 2. Paragraph 3 allows for Member States to adopt legislation "delaying, restricting or omitting" the provision of the information to the data subject pursuant to paragraph 2 for public interest, such as public or national security. The Directive does not explicitly impose a duty of notification of the data subjects on law enforcement authorities after their data have been accessed, not even when information can no longer prejudice an ongoing criminal investigation. In addition, Art. 15(3) Police Directive allows for the controller to withhold information from the data subject regarding any refusal or restriction of access, as well as the reasons for such refusal or restriction, if providing this information would undermine any of the aforementioned public interest purposes.

cc) Data Protection Regulation for EU Institutions and Bodies

The Data Protection Regulation for EU Institutions and Bodies applies, according to Art. 2(1), to the processing of personal data by all Union institutions and bodies, that is, eu-LISA, Europol, Eurojust, or the ETIAS Na-

579 According to Art. 2(1) in conjunction with Art. 1(1) the Police Directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It does not, however, apply to Union institutions, bodies, offices and agencies, such as Europol or Eurojust, according to Art. 2(2)(b).

tional Unit (EBCG Agency).[580] The material scope in Art. 2(5) corresponds to that of the GDPR and the Police Directive. Thus, it encompasses data collected under the Interoperability and Eurodac Regulations.

As in the GDPR, Art. 15 Data Protection Regulation for EU Institutions and Bodies contains information to be provided where personal data are collected from the data subject, while Art. 16 refers to situations where personal data have not been obtained from the data subject. The structure and lists of information are almost the same as in the GDPR. Paragraph 2 refers to further information necessary to ensure fair and transparent processing; paragraph 3 to situations where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected. Restrictions to these rights are broader than under the GDPR and contained in Art. 25.

d) *Eurodac Regulation and AMMR*

According to the Eurodac Regulation, asylum applicants, persons registered for resettlement, migrants apprehended in connection with the irregular crossing of an external Schengen border, disembarked following a SAR operation or staying irregularly in a Member State, and beneficiaries of temporary protection from the age of six years are obliged to have their fingerprints and their facial image as well as biographical data taken.[581] Consequently, they must be informed about certain aspects of data processing in Eurodac and the objectives of the AMMR, in accordance with Art. 19, and, if applicable, the objectives of the Resettlement Regulation.[582] While the list of information in Art. 19 AMMR is quite specific, the list in Art. 42 Eurodac Regulation is rather general. It itemises the identity of the controller within the meaning of the GDPR and of their representative, if any, along with the data protection officer's contact details. While the proposals for a Eurodac Regulation initially included a list of purposes for which someone's data would be processed in Eurodac,[583] the law now only requires that the data to be processed in Eurodac be notified to the data subject. It must also provide a clear and intelligible explanation, using plain language, of the fact that Eurodac may be accessed by Member States and

580 Data Protection Regulation for EU Institutions and Bodies.
581 Eurodac Regulation 2024, Art 14, 15, 18, 20, 22, 23, 24 and 26.
582 ibid, Art 42(1)(a).
583 2016 Eurodac Proposal, Art 30; 2020 Eurodac Proposal, Art 30.

Europol for law enforcement purposes.[584] If applicable, the data subjects need to be informed of the fact that a security check shows that the data subject is considered to be a threat to internal security.[585] Furthermore, the recipients or categories of recipients of the data must be disclosed. Where applicable, the obligation to provide fingerprints, the procedure for doing so, the consequences of non-compliance, and the duration for which the data will be stored must also be communicated.[586] The data subject has to be informed about the existence of the right to access, rectification, completion of incomplete personal data, erasure or restriction, as well as the right to receive information on the procedures for exercising those rights. This includes the contact details of the controller and the supervisory authorities.[587] Finally, data subjects need to know about the right to lodge a complaint to the supervisory authority.[588]

Additionally, in case of a data breach, data subjects may be informed of this as held in Art. 34 GDPR.[589] However, if a Member State has evidence to suggest that data were recorded in Eurodac in breach of the Eurodac Regulation, Member States are not obligated to notify the data subject but only check the data concerned and, if necessary, amend or erase them without delay.[590]

These provisions must be interpreted in the light of the above-mentioned principles, such as the principle of transparency. Data subjects must not only be informed; the information must be communicated to them in such a way that they can understand and assess the consequences of the data processing. Data subjects have to be informed "in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[591] For that purpose, a common leaflet with the information mentioned was created by the EU;

584 Eurodac Regulation 2024, Art 42(1)(b).
585 ibid, Art 42(1)(c).
586 ibid, Art 42(1)(d-f).
587 ibid, Art 42(1)(g).
588 ibid, Art 42(1)(h).
589 The Eurodac Regulation seems not entirely clear on this. While it refers in ibid, Art 48(3) to GDPR, Art 33 and 24, in case of a data breach, Eurodac Regulation 2024, Art 40(5), only refers to GDPR, Art 33, which contains notification of the supervisory authority, but not the data subject, in case of a data breach.
590 Eurodac Regulation 2024, Art 40(5).
591 ibid, Art 30(1); Dublin III Regulation, Art 4(2).

Member States can complete it with additional state-specific information.[592] Minors must be informed in an age-appropriate manner.[593] According to the law, information shall be provided "at the time when his or her biometric data are taken".[594]

e) *Interoperability Regulation*

Art. 47(3) Interoperability Regulation holds that persons whose data are recorded in VIS, EES, or ETIAS must be informed about the processing of personal data for the purpose of interoperability, when their individual file is created or updated in one of these databases.[595] However, this is not the case for persons whose data are recorded in Eurodac.[596] Data subjects will receive no information regarding updates in their file.

Besides that, the Interoperability Regulation refers to Art. 13 and 14 GDPR, Art. 12, 13 Police Directive, as well as Art. 15 and 16 Data Protection Directive for EU Institutions and Bodies regarding the right to be informed. These norms are applicable when collecting or processing data, based on the Interoperability Regulation, which includes data recorded under the Eurodac Regulation.[597] According to Art. 47(2) Interoperability Regulation, all information shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand. This includes providing information in a manner that is appropriate to the age of the data subjects who are minors. However, Art. 47(3) Interoperability Regulation states that "[t]he rules on the right to information contained in the applicable Union data protection rules shall apply to the personal data recorded in ECRIS-TCN and processed for the purposes of this Regulation." No mention is made to data recorded in Eurodac. It seems unclear whether the right to information contained in the Interoperability Regulation is intended to apply to Eurodac data at all.

592 Eurodac Regulation 2024, Art 42(3), in conjunction with AMMR, Art 19.
593 Eurodac Regulation 2024, Art 42(2).
594 ibid, Art 42(2).
595 Interoperability Regulation - Borders, Art 47(3).
596 Interoperability Regulation - Judicial Cooperation, Art 47(3); Interoperability Regulation - Borders, Art 47(3).
597 cf section C.II.: The Interoperability Regulations.

2. Scope and Limitations

a) *Informed about What?*

As seen above, the right to information under the Eurodac and Interoperability Regulations includes a range of information that must be provided to data subjects when they provide their biometric data to Eurodac. Certain information outlined in Art. 41(1) Eurodac Regulation is relatively straightforward, such as the identity and contact details of the controller as defined by the GDPR, the contact details of the data protection officer, and the period for which the data will be stored, in accordance with Art. 29 Eurodac Regulation. Such information can be easily and clearly provided for each category of data subjects in a leaflet, as foreseen in the Eurodac Regulation. Regarding other information, whether listed or not in the Eurodac Regulation, and particularly in the Interoperability Regulation, questions arise as to whether, and to what extent, such information must be provided to data subjects. This will be analysed in the following section.

aa) Eurodac Regulation

aaa) *Purposes*

As noted above, the new Eurodac Regulation does not list the purposes of data use among the information that must be provided to data subjects. This is surprising, not only because the GDPR expressly requires that data subjects be informed of the purposes of processing[598], but also because such information was included in the 2016 and 2020 Eurodac Proposals.[599] It is all the more noteworthy given that the purposes of Eurodac have been significantly expanded in the latest revision: Eurodac has evolved far beyond a mere support tool for applying the AMMR.

The principle of transparency is anchored and concretised in the GDPR. It can also, as seen above, be derived from Art. 8 and arguably Art. 7 CFR, as well as Art. 8 and 10 ECHR. It is, accordingly, argued here that the vari-

598 GDPR, Art 13(1)(c), this can also be derived from the transparency principle in Art 5(1)(a) and is stated also in ibid, Recital 63: "Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, […]".

599 2016 Eurodac Proposal, Art 30(1)(a); 2020 Eurodac Proposal.

ous purposes for which Eurodac data can be used must be communicated to the data subject, including the reasons that are not mentioned in the Eurodac Regulation, namely, the use of Eurodac data for the MID.[600]

The question accordingly arises as to how far these purposes need to be explained. The purpose to "assist with the control of irregular immigration to the Union, with the detection of secondary movements within the Union and with the identification of illegally staying third-country nationals and stateless persons for the purpose of determining the appropriate measures to be taken by Member States" or "support evidence-based policy making through the production of statistics", for example, might sound rather abstract to data subjects not familiar with EU information systems. Information has to be provided in an "intelligible" way, which means that it should be understood by an average member of the intended audience.[601] The language should be short and direct, avoiding complicated legal constructions.[602] Data subjects must, at a minimum, understand that their data can be accessed by the police and will be used to generate statistics on the behaviour of migrants accessible not only to national authorities but also to EU institutions. Although not even listed as a purpose, the fact that their data are used to test new technologies within Eurodac should be made known to them. In addition, data subjects should receive the means to inform themselves further, if they wish to do so.

bbb) *Security Flags*

Following the security checks as held in the Screening Regulation, the AMMR and the Asylum Procedure Regulation[603], the fact that a person

600 Where the controller intends to further process personal data for a purpose other than that for which they were collected, the controller shall, according to GDPR, Art 13(3), provide the data subject, prior to further processing, with information on the other purpose and with any relevant further information as referred to in paragraph 2; cf also ibid, Recital 61.
See Eurodac Regulation 2024, Art 35(3) and 39(1).

601 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 7 para 9.

602 Gabriela Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, Oxford University Press 2020) 427.

603 Eurodac Regulation 2024, Art. 17(2)(i), 22(3)(d), 23(3)(e) and 24(3)(f) in conjunction with the Screening Regulation, AMMR and the Asylum Procedure Regulation.

could pose a threat to internal security is recorded in Eurodac if the person is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in Directive (EU) 2017/541 (Terrorism Directive)[604] or in any of the offences referred to in the European Arrest Warrant (EAW) Council Framework Decision[605]".[606] According to Art. 42(1)(c) Eurodac Regulation, the data subject concerned has to be informed about the fact that they are considered to be a potential threat to internal security and that the Member State of origin is obliged to register that fact in Eurodac. What is unclear, though, is which information exactly the data subject has to be provided with.

From the Eurodac Regulation itself it is not clear what information exactly will be stored in Eurodac. It does not provide whether a security flag record is a simple 'tick box' or a free text input system, allowing a national authority to enter information with some discretion.[607] During the Eurodac Regulation's revision process, there has been criticism that this category is not in line with the requirement for clarity and precision, in accordance with the case law of the Court of Justice of the EU.[608] As we know now, the Screening Regulation provides that a health and vulnerability, an identity, and a security check are conducted with specific information considered.[609] A screening form has to be filled out with data on the data subject and results of the screening.[610] With regard to the security check, the form indicates whether the consultation of relevant databases resulted in a hit

604 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism [2017] OJ L88/6 (Directive on Combating Terrorism).

605 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision [2002] OJ L190/1 - Statements made by certain Member States on the adoption of the Framework Decision (EAW Framework Decision).

606 Eurodac Regulation 2024, Art 17(2)(i) and Recital 8. The list of offences covered by this directive is much shorter than was the case with earlier drafts of the new Eurodac Regulation; However, this limitation is offset by the potentially very broad and defined only in ibid, Recital 8, "whether the person has displayed behaviour that results in physical harm to other persons that would amount to a criminal offence under national law".

607 cf Niovi Vavoula, 'Focus on Eurodac: Disentangled from the "Package Approach" but Is It Fit to Fly?' (ECRE 2023) 19.

608 ibid 19; with reference to 'Opinion 1/15 on the Draft Canada-EU PNR Agreement' (n 541), paras 155-163.

609 Screening Regulation, Art 12 and 14-16.

610 ibid, Art 17.

or not.[611] It is unclear whether the form shows which database comparison resulted in a hit and which did not. The security flag may therefore just be 'tick box' information. The Screening Regulation form is part of the information that a data subject who will relocate seems to receive. This is stipulated in Art. 18(3) Screening Regulation, which states that "the third-country national concerned shall be referred to the relevant authorities of the Member States concerned together with the form […]". However, this is not provided for data subjects who applied for international protection or other data subjects who have not applied for asylum.[612]

In addition, the Eurodac Regulation introduces three additional criteria, as listed above, one of which has to apply in order for data subjects to be registered as a potential threat to internal security in Eurodac.[613] This study argues that if a person is violent, unlawfully armed, or there are clear indications of their involvement in a criminal offence, these facts must be documented in detail and supported with evidence.[614] For example, whether someone is 'violent' is a matter of assessment. Such a designation must be supported by evidence in Eurodac, unlike an entry based on a security-relevant list or database. Data subjects should, at the time their biometric data are collected, be informed that a Eurodac entry has been made and should be told on which of the three criteria this decision is based. More detailed information will likely not have to be passed on to the data subject at the time their biometric data are taken – if any information is provided at all. The German National Implementation Plan, the only publicly available plan mentioning details about access to data, states that "information provided to data subjects regarding data stored under the Eurodac Regulation does not extend to matters relevant to security."[615] However, as will be shown in the next chapter, some information should be made accessible to the data subject upon request. It is argued that, when biometric data are collected, data subjects must not only be informed of the existence of a security flag and the criteria underlying the Eurodac entry,

611 ibid, Art 17(h).
612 ibid, Art 18(2), (4).
613 Eurodac Regulation 2024, Art 17(2)(i).
614 cf ibid, Recital 8; see chapter: The Right to Access Information.
615 'Nationaler Implementierungsplan (NIP) für Deutschland' (*Bundesministerium des Innern und für Heimat,* 20 December 2024) 9: "Die Auskunft an die Betroffenen über ihre nach der EURODAC-VO gespeicherten Daten erstreckt sich nicht auf sicherheitsrelevante Belange."

but must also be told that they may obtain additional details concerning the security flag.[616]

ccc) *Recipients*

According to Art. 42(1)(d) Eurodac Regulation, the data subjects have to be informed about the recipients or categories of recipients of their data. A distinctive feature of Eurodac data (or all data in interoperable databases) is that data are not only shared but more often directly accessed by other authorities. According to Art. 4(9) GDPR, "recipient" means a person, authority, agency or another body to which the personal data are disclosed. According to Art. 4(2) GDPR, disclosure means transmission, dissemination, or otherwise making available of data. If an authority gains access to Eurodac data, even if it is just in read-only format, these data have been disclosed to them, which makes them recipients in the sense of the GDPR.

The Eurodac Regulation itself does not entail details on what it understands to be recipients. As mentioned, Art. 4(9) GDPR states that "recipient" means "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not". Art. 4(9) GDPR provides a broad definition of "recipient" that covers essentially any entities or individuals to whom personal data are disclosed or made available.[617] Recipients do not have to be third parties but also include, for example, another department of the organisation of the controller or joint controllers.[618]

However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients, according to Art. 4(9) GDPR. This exception is viewed critically by some scholars.[619] The question then is: do Member States, third countries, Europol, law enforcement authorities, the EBCG Agency, and eu-LISA, all of which are public authorities, fall under

616 ibid, Art 42(1)(g).

617 Luca Tosoni, 'Article 4(9). Recipient' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, Oxford University Press 2020) para 166.

618 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 37; Tosoni, 'Article 4(9). Recipient' (n 617) para 166.

619 Maximilian Hartung, 'Art. 4 - Begriffsbestimmungen' in Jürgen Kühling and Benedikt Buchner (eds), *DS-GVO/BDSG - Datenschutz-Grundverordnung Bundesdatenschutzgesetz: Kommentar* (4th edn, CH Beck 2024), para 7.

the exemption of Art. 4(9) GDPR? This would lead to data subjects not having to be informed about who can access and receive their data at all.

Recital 31 of the GDPR states that "[p]ublic authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law." In some countries, these public authorities are referred to as authorised third parties.[620] This concept primarily covers judicial, police, and tax authorities; it may extend to other entities or individuals entrusted with functions of a public nature, such as customs officers, social security officers and bailiffs.[621] The Modernised Convention 108+ mentions the exception of public authorities entrusted with a "particular inquiry", too.[622] Tosoni argues that the use of the word 'inquiry' in Art. 4(9) GDPR suggests that the authority's request for personal data may have a variety of purposes and does not need to be issued in the context of an enforcement action. He states that nonetheless, the request must be specific (a particular inquiry) and have a legal basis (in accordance with Union or Member State law).[623]

It follows that possible access to Eurodac data by Europol and national law enforcement authorities would probably not have to be communicated to the data subjects if this were not expressly provided for in the Eurodac Regulation.[624] The supervisory authority, as a potential recipient, need not be disclosed to data subjects, since it gains access only in the context of specific investigations or inquiries. Other authorities – such as national visa, immigration, or asylum authorities of Member States, third countries, and eu-LISA – may not fall within the exception in Art. 4(9) GDPR, as they are not entrusted with a "particular inquiry" but rather hold broader mandates that permit regular access. It may also be argued, however, that

620 In French, "tiers autorises" as stated, e.g. in Livre des procédures fiscales [1982] (French Tax Procedure Code).

621 Tosoni, 'Article 4(9). Recipient' (n 617) para 167, with reference to: Commission Nationale de l'Informatique et des Libertés, 'Besoin d'aide' (*cnil.fr*) <https://www.cnil.fr/fr/cnil-direct>.

622 Modernised Convention 108+, 'Explanatory Report to the Modernised Convension 108+', para 23.

623 Tosoni, 'Article 4(9). Recipient' (n 617) 167.

624 Eurodac Regulation 2024, Art 42(1)(b).

the processing of an asylum application constitutes a "particular inquiry," in which case none of the above recipients would need to be communicated to the data subject.

ddd) *Transfer of Data to Third Countries*

Under the revised Eurodac Regulation, the possibilities to transfer data to third countries, international organisations, or private entities have been extended. Personal data exchanged between Member States following a hit obtained for law enforcement purposes can be transferred to third countries, if there is no "real risk"[625] that as a result of such transfer the data subject may be subjected to any violation of their fundamental rights, according to Art. 49(2) Eurodac Regulation *e contrario*.

Data can furthermore be transferred for the purpose of return. In this case, personal data obtained following a hit in Eurodac can be transferred or made available to third countries. The conditions for such a transfer are, first, that the Member State of origin agrees. Second, the data are transferred or made available solely for the purpose of identifying and issuing an identification or travel document to an illegally residing third-country national for the purposes of return, and the individual concerned has been informed that their personal data may be shared with the authorities of a third country.[626] While the 2016 Proposal for a Eurodac Regulation stipulated that the receiving country must explicitly agree that the data would only be used for the purpose for which they were provided and that the data would be deleted when it was no longer justified to retain them, these provisions have not been incorporated into the current Eurodac Regulation.[627]

In any case, transfers of personal data to third countries shall not prejudice the right contained in the Eurodac Regulation, in particular as this regards non-refoulement.[628]

The transfer of data under the Eurodac Regulation is not tied to the condition that the receiving state provides a certain level of data protec-

625 Under the 2016 Eurodac Proposal, Art 35 it was a "serious risk".
626 Eurodac Regulation 2024, Art 50(1) and (3).
627 2016 Eurodac Proposal, Art 38(1).
628 cf Eurodac Regulation 2024, Art 49(4) and 50(5).

tion.[629] Unlike under the GDPR, also no "legally binding and enforceable instrument between public authorities or bodies" or a similar mechanism has to be in place.[630] Third countries of return are also often not subject to adequacy decisions adopted by the Commission under the GDPR.[631] Since the Eurodac Regulation does not request a data protection agreement of a third country, as was suggested in the Eurodac Proposal 2016[632], no real data protection standards with regard to third countries seem to be in place.

Data protection measures regarding data transfers in accordance with the GDPR generally apply to Eurodac data as *lex generalis*.[633] The Eurodac Regulation states that "as an exception to the requirement of an adequacy decision or appropriate safeguards, the transfer of personal data to third-country authorities pursuant to this Regulation should be allowed for the purpose of implementing the return policy of the Union, and it should be possible to use the derogation provided for in [Art. 49 GDPR], provided that the conditions laid down in that Regulation are met." There is only

629 According to GDPR, Art 45 "[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection." GDPR, Art 46 continues, "[i]n the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." However, these safeguards have to be much stricter than an agreement by the State, as it is foreseen in the Eurodac Regulation. Under the GDPR, safeguards can be e.g. a legally binding and enforceable instrument between public authorities or bodies; an approved code of conduct pursuant to GDPR, Art 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or an approved certification mechanism pursuant to GDPR, Art 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. Only under certain conditions, according to GDPR, Art 49 can data be transferred in the absence of an adequacy decision pursuant to Art 45(3), or of appropriate safeguards pursuant to Art 46, amongst which one is the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

630 ibid, Art 46(a); see in contrast Case T-354/22 *Thomas Bindl v European Commission* [2025], regarding unlawful data transfer of an Eu citizen to the US.

631 Eurodac Regulation 2024, Recital 85.

632 2016 Eurodac Proposal, Art 38(1)(b).

633 See regarding *lex generalis/specialis* chapter: The Right to Information; see also Eurodac Regulation 2024, Recital 84ff.

one reason for derogation stated in Art. 49(1)(b) GDPR, which is applicable to situations under the Eurodac Regulation: the transfer is necessary for important reasons of public interest. As examples for such interests, the GDPR states cases of international data exchange between competition authorities, tax, or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport.[634] One may ask whether the return of rejected asylum seekers in individual cases should be considered an "important reason of public interest". It would certainly be questionable if the majority of the EU's return practice is based on a derogation in the GDPR. This would massively restrict data protection for asylum seekers in the EU.

Third countries are recipients in the sense of Art. 4(9) GDPR. Hence, data subjects should at least be informed that their data may be sent to other countries after a hit for law enforcement purposes. The Eurodac Regulation rightly provides that for return purposes, data subjects must be informed that their data may be transferred to third countries. This information must be given to the data subjects when they submit their fingerprints.[635] It can be argued, however, that it should be repeated shortly before data are sent to the third country. The Art. 29 Working Party demanded, with regard to the transfer of information under the GDPR, that data protection safeguards taken by the receiving state should be specified and provided to the data subjects.[636] In accordance with the principle of fairness, the information regarding data transfers should be as meaningful as possible to data subjects.[637] These demands are equally valid with regard to the Eurodac Regulation. Furthermore, data subjects should be provided with the explicit assurance from the third country that their data will be protected. As we have seen above, many data transfers will be based on the derogation in Art. 49 GDPR. Thus, no other data protections are in place. Such confirmation – even if not aligned with recognised EU data-protection standards – could at least assist the data subject in enforcing their data-protection rights in the third country concerned.

634 GDPR, Recital 112.
635 Art. 42(2) Eurodac Regulation 2024.
636 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 38.
637 ibid.

eee) *Data Breach*

As was mentioned above, in case of a data breach, data subjects may be informed of this, although the Eurodac Regulation is not entirely clear on this. While Art. 48(3) Eurodac Regulation addresses data security and refers to Art. 33 and Art. 34 GDPR in the context of a data breach, it is important to note the distinctions between these articles. Art. 34 GDPR establishes the obligation to notify data subjects under certain circumstances. In contrast, Art. 40(5), sentence 1 Eurodac Regulation, which pertains to access to and the rectification or erasure of data recorded in Eurodac, only references Art. 33 GDPR. This provision contains the obligation to notify the supervisory authority, but not the data subject, in case of a data breach. If a Member State possesses evidence indicating that data have been recorded in Eurodac in violation of the Eurodac Regulation, it is not required to notify the data subject. Instead, according to Art. 40(5), sentence 2 Eurodac Regulation, the Member State must review the relevant data and, if necessary, amend or erase it without delay. This seems hardly compatible with the transparency principles. At least in cases where there is a possibility that data subjects can derive a claim, such as a claim for damages, from the unlawful collection or processing of their data, the data subject should be informed.

bb) Interoperability Regulation

The biggest change and the biggest challenge regarding the right to information is the coming interoperability between the various EU information systems, including Eurodac. Up until now, data collected under the Eurodac Regulation are only stored in the Central System of the Eurodac information system. This will change, once the interoperability system is operable. Up to 27 data items are collected of data subjects, if available, of which eight are stored in the CIR and the remaining in the Central System.[638] The CIR creates an individual file for each person that is registered in Eurodac.[639] For the purpose of multiple-identity detection, the MID also creates an identity confirmation file, with, among other data, links, and a

638 Eurodac Regulation 2024, Art 4(2) and 17.

639 Interoperability Regulation - Judicial Cooperation, Art 17(1) in conjunction with ibid, Art 18(1) and ECRIS-TCN Regulation, Art 5; see fn 452.

reference to the information system wherein the linked data are held.[640] The sBMS stores biometric templates obtained from the biometric data that are stored in the CIR and SIS. By doing so, it enables the querying with biometric data across several EU information systems.[641] In short, data collected under the Eurodac Regulation will be stored in all three interoperability systems.

As noted above, Art. 47 Interoperability Regulations contain a general right to be informed, referring to Art. 13 and 14 GDPR, Art. 12 and 13 of the Police Directive, and Art. 15 and 16 of the Data Protection Directive for EU Institutions and Bodies. Art. 47(3) Interoperability Regulation, which applies to Eurodac data, provides that the rules on the right to information contained in the applicable Union data protection legislation shall apply to personal data recorded in ECRIS-TCN, without explicitly mentioning Eurodac.[642] The Commission's original proposal of 2017[643] and the Amended Proposal for the Interoperability Regulation of 2018 explicitly held the right to information with regard to Eurodac data in Art. 46(2).[644] It stated that "[p]ersons whose data is recorded in Eurodac or [the ECRIS-TCN system] shall be informed about the processing of data for the purposes of this Regulation in accordance with paragraph 1 when: (d) [an application for international protection is created or updated in Eurodac in accordance with Article 10 of the Eurodac Regulation]." This right to information, later codified in Art. 47, was amended in its formulation in 2019 following the outcome of the European Parliament's first reading.[645] The changes were

640 Interoperability Regulation - Judicial Cooperation, Art 25(1) in conjunction with ibid, Art 34; For the meaning of multiple-identity detection a set of at least the fingerprint data, facial image, names, nationalities, date and place of birth have to be recorded in the CIR (Interoperability Regulation - Judicial Cooperation, Art 27(1)).

641 Interoperability Regulation - Borders, Art 13(1); Interoperability Regulation - Judicial Cooperation, Art 13(1).

642 Interoperability Regulation - Judicial Cooperation, Art 47(3).

643 Proposal for an Interoperability Regulation 2017 - Judicial Cooperation, Art 46.

644 Amended Proposal, capital proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation] [2018] COM(2018)480 (Amended Proposal for an Interoperability Regulation – Judicial Cooperation), Art 46.

645 7751/19 from General Secretariat of the Council, 'Amended Proposal for a Regulation of the European Parliament and of the Council on Establishing a Framework

kept in later versions; they are not addressed in the legislative material.[646] Art. 47(1) Interoperability Regulation states that "persons whose data are collected" have a right to be informed. Persons are included whose data are collected in Eurodac. It is unclear whether the exclusion of any mention of Eurodac in paragraph three of the provision is to be understood as a limitation of paragraph one. It is, however, a clear deviation from the Art. 46(2) of the (Amended) Interoperability Proposal. The right to information is derived from human rights law in Art. 7 and 8 CFR, as described above, and enshrined in Art. 13 GDPR. These provisions are applicable to data subjects recorded in Eurodac. There is no apparent reason why persons whose data are recorded in Eurodac should be excluded from the right to information. No security-related or important public reasons for a limitation seem to apply. Art. 47(3) Interoperability Regulation should thus not be interpreted as a limitation to paragraph one. Data subjects, it is argued here, whose information is recorded in Eurodac retain the right to information under the Interoperability Regulation.

Both Interoperability Regulations grant a specific right to be informed about a red link, provided that no limitations are necessary to protect security and public order, prevent crime, or ensure that ongoing national investigations are not compromised.[647] These limitations have been criticised by the EDPS as inconsistent with Art. 13(3) Police Directive.[648] They were nevertheless retained in the version adopted by the EU's legislator.

The Interoperability Regulations do not describe how such information must be provided to data subjects. They do not refer to Art. 12 GDPR, which states that "[t]he controller shall take appropriate measures to pro-

for Interoperability between EU Information Systems (Police and Judicial Cooperation, Asylum and Migration) and Amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the Field of Law Enforcement], Regulation (EU) 2018/XX [the ECRIS TCN Regulation] and Regulation (EU) 2018/XX [the Eu-LISA Regulation] - Outcome of the European Parliament's First Reading (Strasbourg, 15 to 18 April 2019)' (25 April 2019).

646 Neither FRA, in: 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71), nor the EDPS in: EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (2018), addressed these changes, as their opinions were formulated in 2018, before the changes in the text occurred.

647 Interoperability Regulation - Judicial Cooperation, Art 32(4); Interoperability Regulation - Borders, Art 32(4).

648 EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), para 117.

vide any information referred to in Art. 13 and 14 [...] to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. [...]".[649] It has been established that the GDPR[650] is considered *lex generalis* in relation to the more specific data protection provisions contained in the Interoperability Regulation.[651] The Interoperability Regulations state that it is important that persons whose data are processed through [the interoperability] components can effectively exercise their rights as required under the GDPR, the Police Directive, as well as the Data Protection Regulation for EU Institutions and Bodies.[652] Art. 12 GDPR should therefore be applied. The question remains: What specific changes occur regarding the processing of Eurodac data due to the Interoperability Regulation? Additionally, what specific information must be communicated to data subjects?

aaa) *The Interoperability System and Automated Processing in the MID*

As was already explained, personal data collected under the Eurodac Regulation are now stored not only in the Central System but also the CIR,[653] the MID,[654] and the sBMS.[655] In the MID, links between different data sets are created in an automated process for the purpose of multiple-identity detection. This constitutes automated decision-making within the meaning

649 Similar provisions are included in the Police Directive, Art 11; Data Protection Regulation for EU Institutions and Bodies, Art 14.

650 Or, with regard to police authorities, the Police Directive; or the EU Institution, the Data Protection Regulation for EU Institutions and Bodies.

651 See chapter: The Right to Information; Eurodac Regulation 2024, Recital 77; Interoperability Regulation – Judicial Cooperation, Recital 53.

652 Interoperability Regulation - Borders, Recital 69; Interoperability Regulation - Judicial Cooperation, Recital 69.

653 Eurodac Regulation 2024, Art 12(1). The CIR creates an individual file for each person that is registered in Eurodac Art 17(1), in conjunction with Interoperability Regulation - Borders, Art 18(1) and ECRIS-TCN Regulation, Art 5.

654 Eurodac Regulation 2024, Art 12(2), in conjunction with according to Interoperability Regulation - Judicial Cooperation, Art 27(1).

655 Interoperability Regulation - Judicial Cooperation, Art 13(1); Interoperability Regulation - Borders, Art. 13(1).

of data protection law.[656] Data subjects must, according to Art. 13(2)(f) GDPR, in conjunction with Art. 22 GDPR, be informed when the basis of a decision is solely automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.[657] Art. 13(2)(f) GDPR states that "at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject"[658] should be provided. This means that data subjects have to be informed about the logic involved, the significance, and the envisaged consequences of data processing in the MID.

It should be noted that Eurodac's purposes do not include the detection of multiple identities. This renders the processing of Eurodac data in the MID questionable. At a minimum, data subjects should be informed of this change in the purpose of data processing.[659] Recital 31 GDPR states that "[w]here the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide

656 EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646) 21 para 86.

657 Such effects are present, for instance, where processing results in potential discrimination, in loss of opportunity (not being selected for a job interview), increased insurance rates [etc.], according to Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602) 429ff; cf also Alessandra Silveira, 'On Inferred Personal Data and the Difficulties of EU Law in Dealing with This Matter' (*Blog of Unio*, 19 March 2024) <https://officialblogofunio.com/2024/03/19/editorial-of-march-2024/#more-6318>.

658 Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 53; without reference to the phrase "at least", Feiler, Weigl and Forgo, 'Article 13 - Information to be provided where personal data are collected from the data subject' (n 575) 109, para 30, argue that meaningful information about the logic involved must also be provided in cases other than automated decision-making to the extent such information is "necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed" as provided in Recital 60 sentence 2 GDPR; cf also Case C-673/17 *Planet49 GmbH* [2019] Opinion of AG Maciej Szpunar, para 78: "Although the duration of the processing of the data is not included as part of that information, it is, however, clear from the words 'at least' in Data Protection Directive 95/46/EC, Art 10, that that information is not listed exhaustively".

659 The principle of purpose limitation is laid down in GDPR, Art. 5(1)(b) and Art. 6(3), (4). The GDPR provides in Art. 13(3) that the controller must inform the data subject about the use of data for new purposes before any further processing of the collected data.

the data subject prior to that further processing with information on that other purpose and other necessary information." This should apply with regard to Eurodac used in the MID, too.

From the phrase "at least" in Art. 13(2)(f) GDPR, some scholars conclude a duty to provide information about the logic involved in other cases of profiling, which are not intended to lead to automated decision-making.[660] This may occur, for example, when statistics generated using Eurodac data are employed in an algorithm to identify security risks, irregular migration, or high epidemic risk (such as under ETIAS screening rules), effectively resulting in profiling.[661] With regard to the logic involved in automated decision-making and digitised profiling, the requirement for the information provided to be comprehensible is particularly important.[662] Information must be presented in a manner that enables the data subject to genuinely understand both its content and the rationale underlying its construction.[663] A controller who is not able to explain in a meaningful way to the data subject the logic involved in an automated decision-making or profiling technique cannot use it in a legally compliant way.[664] The controller further has to inform the data subject about what they should expect to happen as a result of a [solely] automated decision-making process.[665]

---

660 cf fn 658.

661 ETIAS Regulation, Art 33.

662 cf GDPR, Art 12(1) information has to be provided in a "a concise, transparent, intelligible and easily accessible form"; Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 55a; similar also: Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), no 10, and Dix, 'Article 15 - Right of Access by the Data Subject' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection Regulation: Article-by-Article Commentary* (1st edn, Bloomsbury Publishing 2023), no 19, where he states that the right to an explanation of automated decision-making, is the only appropriate response to the informal asymmetry between the State and the data subject.

663 Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602) 430: "The 'logic involved in the processing should be a description of the rationale used to build that specific automated decision-making process, and not the algorithm used, nor lines of code used, nor how machine-learning or algorithmic decision-making work in general."; Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 55a.

664 Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 16.

665 Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602) para 430.

It can therefore be argued that, at a minimum, data subjects should be informed that their data are continuously cross-checked to detect potential identity fraud and may feed into an algorithm designed to indicate to authorities which individuals may pose a security, irregular migration, or high epidemic risk. Furthermore, data subjects should be made aware that, under the Interoperability Regulations, comprehensive statistics on migration patterns will be compiled.[666] Data subjects also need to understand – at least at a basic level – the functions of the other interoperability systems, including ESP, CIR, and sBMS, and the purposes for which their data are processed within these systems.[667] With regard to red links, the above-mentioned security exception to the right to information should be limited in time until the point when the risk that triggered the limitation no longer exists.

bbb) *Cross-Checking Data*

Eurodac's Central System is connected to the ESP in order to enable the automated processing by the ETIAS.[668] Whenever an application file is created in ETIAS, automated processing with Eurodac verifies if the data corresponds to an event foreseen in the ETIAS Regulation,[669] such as whether the applicant is registered in Eurodac.[670] Besides the automated processing, ETIAS National Units can consult Eurodac manually for the purpose of examining applications for travel authorisation.[671] Similar mechanisms exist with regard to VIS. Application files for Schengen visas recorded in VIS are automatically compared against Eurodac data.[672] For the purpose of manually verifying hits triggered by VIS queries and for deciding on visa applications, visa authorities have access to Eurodac.[673] Data subjects should be informed about the automatic comparison with

666 cf Interoperability Regulation - Border, Art 39; Interoperability Regulation – Judicial Cooperation, Art 39.
667 GDPR, Art 5(1)(a) and 13(1)(c).
668 referred to in the ETIAS Regulation, Art 11.
669 ibid, Art 20.
670 ibid; Eurodac Regulation 2024, Art 8. If this procedure results in a hit, the ETIAS Central Unit and ETIAS National Unit may have access to personal data for further verifications.
671 Eurodac Regulation 2024, Art 9.
672 Amendment to the VIS Regulation 2021, Art 9(a); Eurodac Regulation 2024, Art 11.
673 Amendment to the VIS Regulation 2021, Art 9(c); Eurodac Regulation 2024, Art 11.

ETIAS and VIS, as this is a key purpose of the data processing. They should also receive information regarding the recipients of their data, specifically the authorities that have access to their personal information.[674]

In general, data subjects need to understand that once their data are recorded in Eurodac, they are fed into a system where they will be constantly cross-checked with other data, be it for law enforcement or migration law purposes. This lies at the core of interoperability; data subjects must be made aware of it when they provide their data. They should also know that their data are (with some specific exceptions for VIS, EES, ETIAS, and Europol) not transferred or made available to third countries, international organisations, or private parties, with the exception of Interpol.[675]

Some scholars argue that in cases of ongoing data processing, the data subjects must be informed regularly.[676] This is an important point in the context of interoperability. Data subjects should be informed about the use of their data and their rights not only during but also after an asylum procedure has been completed. Since, as will be shown below, many data subjects do not receive adequate or correct information during asylum, return, or Dublin procedures, they must at least be able to understand interoperability at a later stage. As noted above, a data subject should never be taken by surprise regarding the purposes for which their personal data are processed.[677] It is doubtful whether this promise can be kept under the interoperability system. Even in the context of Eurodac, data subjects are frequently not fully informed of all aspects of data processing. They often struggle to understand the information provided, as will be demonstrated in the next chapter. Field reports indicate that this problem is especially pronounced when the information system in question serves multiple purposes and processes.[678]

674 GDPR, Art. 5(1)(a) and 13(1)(c), (e); also, FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (2017) 33.

675 Interoperability Regulation - Borders, Art 50, in accordance GDPR, Art 13(1)(f); Police Directive, Art 13(2)(c).

676 cf Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 6 para 4; Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 7.

677 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 23 - 24, para 45.

678 FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 46.

ccc) *Encompassing Access by the Police*

Police authorities will have access to CIR data, including Eurodac data, in situations where they are unable to identify an individual, have doubts about the identity information provided by that individual or their travel documents, or when a person is unable or refuses to cooperate.[679] In these circumstances, an authorised police authority can, solely for the purpose of identifying a person, query the CIR with the biometric data taken live during an identity check, provided that the procedure was initiated in the presence of that person. [680] The police also have access to certain biographic data and information on travel documents.[681] In this regard, police authorities do not fall within the exception provided by Art. 4(9) GDPR, noted above, and must be treated as recipients about whom data subjects are to be informed pursuant to Art. 13(1)(e) GDPR. Since data subjects must also be informed of the purposes of data processing under Art. 13(1)(c) GDPR, they should be made aware that the police may access their data to carry out identity checks in cases of doubt.

ddd) *Controllers with Regard to Eurodac Data*

According to Art. 42(1)(a) Eurodac Regulation and Art. 47(1) Interoperability Regulation in conjunction with Art. 13 GDPR, data subjects must be informed of the identity of the controller in accordance with the GDPR.[682] However, under the new Interoperability Regulations, the controller's identity is not always clear.[683]

Art. 40 Interoperability Regulation indicates that in the Member States, the same competent authorities who function as the controllers for the

679 Interoperability Regulation - Judicial Cooperation, Art 20(1).

680 ibid, Art 20(2).

681 ibid, Art 20(3) in conjunction with ibid, Art 18(1).

682 GDPR, Art 4(7): "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

683 Art. 29 WP, 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (2018) 18/EN WP266 15.

underlying system (e.g., Eurodac) will also have responsibility for the processing of the same personal data that are stored in the CIR, sBMS, and MID. With regard to data in the MID, the Interoperability Regulation adds that the EBCG Agency shall be considered a data controller in addition to the Member States authorities.

As stated by the Art. 29 Working Party, this allocation of responsibilities does not clarify whether all competent authorities should be regarded as joint controllers under Art. 26 GDPR. This consideration applies both within the same Member State, encompassing all relevant controllers of the underlying data processing systems, and at the EU level, involving all pertinent competent authorities regarding the processing of data within the CIR, the shared BMS, and the MID. Indeed, Art. 26 GDPR foresees that "where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".[684] It is not entirely clear who bears responsibility for the data processed in the CIR, MID, and sBMS. Consequently, it is not possible to fully inform a data subject of the identity of the controller. From the perspective of the principle of transparency, the data subject should be provided with two key pieces of information: first, who may process their data (i.e., each controller should be identified); and second, whom the data subject should contact in order to make inquiries or exercise their access rights.

eee) *New Functions*

The question of potential new functions could also be raised in relation to the Eurodac Regulation, but it is particularly salient in the context of interoperability. Are data subjects informed about the expansion of interoperability, and if so, by what means? It appears likely that, once interoperability becomes operational, new functions, tools, or changes in the use and processing of data may be introduced.[685]

684 ibid.

685 cf e.g., Amended Proposal for an Interoperability Regulation - Judicial Cooperation, which suggests and update regarding the Prüm framework, by linking to interoperability the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (Passenger Name Record (PNR) and Directive, and Regulations on Advance Passenger Information (API), which will update the the Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data; see also

Art. 13(3) GDPR provides that the data controller must inform the data subject of any new purposes for which their data will be used, prior to any further processing. This allows data subjects the opportunity to challenge such further use of their data.[686] Scholarly opinion holds, however, that if the re-purposing of data is based on Union or Member State law, no additional duty to inform arises.[687] Neither data subjects residing in the EU nor those who have left the EU at the time that new interoperability or Eurodac functions are implemented will be notified of the new purposes for which their data are being used. This raises concerns about whether new purposes for data processing can lawfully be introduced without notifying the data subjects, particularly given the large volumes of highly sensitive data collected under the Eurodac Regulation. Even if the EU sought to inform data subjects – for instance, when implementing additional uses of facial recognition software – practical challenges, especially regarding data subjects outside the EU, would make this extremely difficult.

b) *Informed When?*

aa) Asylum, Resettlement, Temporary Protection or Apprehension in an Irregular Situation

Providing information in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly.[688] Paragraph 2 of Art. 42 Eurodac Regulation provides that information shall be given "at the time when his or her biometric data are taken". According to the Interoperability Regulation, information needs to be provided to data

Border Violence Monitoring Network (BVMN), 'Decoding Balkandac: Navigating the EU's Biometric Blueprint' (2023); 'Submission to European Commission Consultation on "Security-Related Information Sharing"' (*Statewatch*, 29 March 2023) <https://www.statewatch.org/analyses/2023/submission-to-european-commission-consultation-on-security-related-information-sharing/>.

686 Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 64.

687 Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 13.

688 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 15, para 27.

subjects "at the time that such data are collected".[689] Similarly, the GDPR states in Art. 13(1) that information has to be provided "at the time when personal data are obtained". These provisions do not explicitly require that information be provided to data subjects prior to the submission of their personal data. Nevertheless, the right to information is grounded in the principle of transparency set out in Art. 5(1)(a) GDPR, Art. 7 and 8 CFR, and Art. 8 and 10 ECHR. Accordingly, data subjects must be aware of and able to understand the consequences and risks of providing their personal data. They must also be informed of their rights in order to exercise them effectively.[690] The information in Art. 13 GDPR must therefore be provided "prior to, rather than after, sign-up",[691] or at least simultaneously, but never "post factum".[692] Since it is not possible to provide information and collect fingerprints simultaneously, data subjects must receive the relevant information prior to submitting their fingerprints.[693] Because of the complexity and the far-reaching consequences of the AMMR and Eurodac systems, even more so after interoperability has become operational, data subjects should be given enough time to study the information they receive. In practice, this is often not the case.

In a study by the Eurodac Supervision Coordination Group (SCG) on the exercise of data subjects' rights in relation to Eurodac, some Member States stated that they provide information to asylum seekers at the time of filing the application; others inform just before fingerprints are taken. One country admitted that it only makes information available on the homepage

689 Interoperability Regulation - Borders, Art 47(1); Interoperability Regulation - Judicial Cooperation, Art 47(1).

690 Roßnagel, 'Artikel 5 - Grundsätze Für Die Verarbeitung Personenbezogener Daten' (n 521); Cécile de Terwangne, 'Article 5 - Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, Oxford University Press 2020) 314.

691 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568), 13 fn 29.

692 Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602); Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522).

693 The question arises whether asylum seekers should have the option not to provide their fingerprints after they have received the information. This question is closely related to the question of whether there is a right to choose the country in which one seeks asylum. For this, see fn 833.

of the system used for editing the results, which is available to persons whose fingerprints are already taken.[694]

Another study by the EU Commission on Dublin III found that only five Member States provide information before an application is lodged,[695] another three when the application is made,[696] and five when registering data.[697] In the majority of Member States, information is provided when the application is signed by the applicant[698] or after the lodging of an application.[699]

Field research in a study from the European Fundamental Rights Agency (FRA) shows different practices. In Sweden, for example, the authorities provide some information orally when taking fingerprints but full information when the asylum application is registered. In Spain, apprehended migrants are only informed that their fingerprints will be registered in a database, without specifying which database, its purposes, or the data subjects' rights, unless a person asks.[700] In various countries, the authorities first take fingerprints (and do a Eurodac search) without giving any information on fingerprinting or Eurodac. Only during a later stage will data subjects be informed about the consequences of the fingerprinting.[701]

Providing information belatedly contravenes the requirement of transparency. Data subjects have a right to understand the implications of submitting their biometric data. One could argue that, upon irregularly crossing an external Schengen Area border, a data subject's personal data –including fingerprints and facial images – must be registered regardless of whether they have applied for asylum.[702] Accordingly, the time at which information is provided cannot be considered decisive. However, the trans-

694 Eurodac Supervision Coordination Group (SCG), 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (2019) 4 Q1.

695 DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (European Commission (EC) 2016) Final Report 9: DE, FR, IE, PL, SI.

696 ibid 9: AT, CY, EL.

697 ibid 9: BE, BG, CZ, DK, LU.

698 ibid 9: BE, BG, CZ, DK, LU.

699 ibid 9: DK, HU, LT, LV, CH, NO.

700 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 32.

701 ibid 34; ECRE, 'Border Procedures: Not a Panacea' (2019) Policy Note #21, 3; Martin Wagner and Caitlin Katsiaficas, 'The State of Play of Schengen Governance: An Assessment of the Schengen Evaluation and Monitoring Mechanism in Its First Multiannual Programme' (EU Parliament, LIBE Committee 2020) PE 658.699 28.

702 Eurodac Regulation 2024, Art 22, 23 and 24; see also Screening Regulation.

parency requirement is rooted in the right to human dignity.[703] It must be emphasised that data subjects under the Eurodac Regulation do not provide legal consent to the processing of their data, as they are not free to object to such processing.[704] Compelling individuals to provide facial images, fingerprints, and other personal data to foreign authorities –who may retain them for years without informing the data subject in advance of its use – appears fundamentally incompatible with the dignified treatment of human beings. Accordingly, information should be provided as early as possible and always prior to the collection of a person's personal data.

bb) Take-Back Procedures

In 2023, the Advocate General at the Court of Justice of the European Union, Juliane Kokott, delivered her Opinion concerning the joined cases C-228/21, C-254/21, C-297/21 and C-328/21. The cases concerned applicants who claimed asylum in a Member State and then travelled to Italy, where they were subject to take-back requests under the Dublin III Regulation (replaced by the AMMR). The questions posed included, among other things, whether the obligations to provide information outlined in Art. 4 Dublin III Regulation (replaced by Art. 19 AMMR) and Art. 29 Eurodac Regulation 603/2013 (replaced by Art. 42 Eurodac Regulation 2024), as well as the obligation to conduct a personal interview under Art. 5 Dublin III Regulation (replaced by Art. 22 AMMR), apply in take-back procedures.[705]

703 cf Dupré, 'Article 1 - Human Dignity' (n 79); Dignity is also mentioned in Eurodac Regulation 2024, Art 13(1)(b), which states that Member States must ensure that the data collected fully respect the human dignity of the person.

704 *Michael Schwarz v Stadt Bochum* (n 547), para 32: "First of all, concerning the condition requiring the consent of persons applying for passports before their fingerprints can be taken, it should be noted that, as a general rule, it is essential for citizens of the Union to own a passport in order, for example, to travel to non-member countries and that that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004. Therefore, citizens of the Union wishing to make such journeys are not free to object to the processing of their fingerprints. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing."

705 According to Joined Cases C-228/21, C-254/21, C-297/21, C-315/21 and C-328/21 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* [2023] Opinion of AG Juliane Kokott, paras 70 and 71, in the take-back procedure, a distinction must be drawn between two situations: First, that procedure is applicable to the situation of persons who lodged

The Advocate General concluded that Art. 4 Dublin III Regulation must be interpreted as meaning that the obligation to provide the information listed there applies in take-back cases, as soon as an application for international protection is lodged.[706] She also stated that a selective obligation to provide information in the take-back procedure, as proposed by the Commission and Italy, appears to be inconsistent with the objectives of the Dublin III Regulation and is difficult to implement in practice.[707] She added that issuing the common leaflet, no matter if a new application was lodged or not, would simply be a good administrative practice that Member States are able to employ.[708]

With regard to Art. 29 Eurodac Regulation 603/2013, the Advocate General stated that it is common ground that the obligation to issue the common leaflet, as established in Art. 29, also applies in the context of the take-back procedure. This is true both whenever a new application for international protection is lodged in the second Member State[709] and if a person is illegally staying in a Member State.[710,711] The obligation to provide information established in Art. 29 Eurodac Regulation 603/2013 aims to clarify to the individuals concerned the purpose of data processing and the methods employed under the Eurodac Regulation.[712] The Advocate General concluded that Art. 29, in conjunction with Art. 9(1) and Art. 17(1) Eurodac Regulation 603/2013, should be interpreted to mean that the obligation to provide the specified information applies as soon as an application for

---

an application in a first Member State and subsequently left that Member State before the procedure for determining the Member State responsible had even been concluded (Regulation Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in one of the Member States by a Third-Country National or a Stateless Person [2013] OJ L180/322 (Dublin III Regulation, Art 20(5)). Second, the take-back procedure is applicable to the situation of persons who, during the substantive examination of their application or following its rejection by the Member State responsible, move to another Member State and, there, lodge another application or stay without a residence document (ibid, Art 18(1)(b) to(d)).

706 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 705), Opinion of AG Kokkott, para 101.

707 ibid, para 80.

708 ibid, para 100.

709 Eurodac Regulation 2024, Art 19(1).

710 ibid, Art 17(1).

711 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 705), Opinion of AG Kokott, para 116.

712 ibid, para 118.

international protection is first lodged with a Member State. This obligation also extends to take-back and take-charge procedures.[713]

The ECJ later decided in the same joined cases C-228/21, C-254/21, C-297/21, C-315/21 and C-328/21 that the literal interpretation of Art. 4 Dublin III Regulation requires the common leaflet to be provided as soon as an application for international protection is lodged, regardless of whether or not it is a first application.[714] A literal interpretation of Art. 29 Eurodac Regulation 603/2013 also requires that the common leaflet be provided to any third-country national or stateless person found irregularly staying in a Member State, whose fingerprints are taken and transmitted to the Central System. The provision of the leaflet must occur no later than the time of transmission, regardless of whether the individual has previously lodged an application for international protection in another Member State.[715] The Court then examined the extent to which the determination of the responsible Member State is necessarily definitive in the event of a take-back and concluded that this may not always be the case. It follows that Art. 4 Dublin III Regulation and Art. 29 Eurodac Regulation 603/2013 must be interpreted as requiring the provision of the specified information – particularly the common leaflet – in multiple contexts. This includes the initial application for international protection and the take-charge procedure, as well as subsequent applications for international protection and circumstances that may give rise to take-back procedures.[716]

cc) Law Enforcement Access and Hits

aaa) *Eurodac Regulation*

Art. 42(1)(b) Eurodac Regulation states that data subjects have to be informed of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes.[717] The question is: when do data

713 ibid, para 121.

714 Joined Cases C-228/21, C-254/21, C-297/21, C-315/21 and C-328/21 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* [2023] C/2024/695, para 80.

715 ibid, para 84.

716 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), para 102.

717 This provision differs from the GDPR, The definition of "recipients" in GDPR, Art 4, covers controllers and processors, but not public authorities, as seen in GDPR

subjects have to be informed about this? From the fact that Art. 42(2) Eurodac Regulation provides that information shall be given "at the time when his or her biometric data are taken", one could conclude that no further information on the use of the data by law enforcement authorities must be given to the data subject later on. However, what happens, one might ask, if traces of a fingerprint, a so-called latent fingerprint,[718] are found at a crime scene? Or a camera records the face of a suspect in connection with a crime that matches a facial image recorded in Eurodac? Will the potential suspect be informed of this match? Or will they only be informed when they are summoned for questioning as a suspect? Will their data in the police files be deleted, if the potential match is not confirmed or they are excluded as potential perpetrator, witness or victim? If not, will they be informed that data has been accessed, but will not be used?

The principle of purpose limitation is central in data protection law. Although it is not stated explicitly in the Eurodac Regulation, it is laid

---

Recital 31: "Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law."; Therefore, it is not required, under the GDPR, to disclose the lawful transfer of personal data to law enforcement authorities of a Member State (Feiler, Weigl and Forgo, 'Article 13 - Information to be provided where personal data are collected from the data subject' (n 575) 107).
It should also be mentioned that access to data in Eurodac for law enforcement purposes is not restricted to persons having reached the age of criminal responsibility. Eurodac Regulation, Art 20 and 21, do not provide for any such limitation. In most EU Member States, the age of criminal responsibility is set at 14 or 15 years. In Ireland, the Netherlands and most parts of the United Kingdom it is set at 12 years (though it is as low as 10 years in Northern Ireland) (European Commission and Directorate-General for Justice, 'Summary of Contextual Overviews on Children's Involvement in Criminal Judicial Proceedings in the 28 Member States of the European Union' (Publications Office 2014)). It is questionable whether such access rights genuinely serve the best interests of the child as required by Article 24 of the CFR. In theory, IT systems have the potential to assist in identifying missing persons particularly unaccompanied children – and victims of crime. However, interviewees noted that the focus continues to be on perpetrators, highlighting the need for a more victim-centred approach ('FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 73. However, since no limitations are in place, children at least have to be informed, that their data can be access by law enforcement authorities.

718 Eurodac Regulation 2024, Art 2(1)(q); ibid, Recital 34.

down in Art. 5(1)(b), Art. 6(3), (4) GDPR, and Art. 4(1)(b) Police Directive. Purpose limitation requires that data may only be used for the purpose for which it was collected. The GDPR provides in Art. 13(3) that the controller must inform the data subject about the use of data for new purposes before any further processing of the collected data. The more the further processing affects the interests of the data subject or the less the data subject could expect it, the earlier the information must be provided.[719] Art. 29 WP even suggest that in the case of ongoing data processing, the controller should remind the data subjects of the information provided at reasonable intervals.[720] FRA argues that a right to be informed when authorities are consulting already stored data might also be derived from the right to good administration.[721]

In the case of access by law enforcement authorities, processing of data is, in principle, not governed by the Eurodac Regulation or the GDPR but by the Police Directive or, in the case of Europol, the Data Protection Directive for EU Institutions and Bodies (as well as the Europol and the Amended Europol Regulation).[722] The Police Directive applies, according to Art. 2(1) and Art. 1(1), to the processing of personal data by national law enforcement authorities.[723] Processing of data, according to the Police

719 Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 20; Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568), 24 para 48.

720 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568), 6 para 5 and 16ff paras 29 ff, derives this from the principle of data processing in good faith (GDPR, Art 5(1)(a).

721 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 39.

722 Data Protection Regulation for EU Institutions and Bodies, Art 1(1); Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation [2016] OJ L135/53 (Europol Regulation); Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's Cooperation with Private Parties, the Processing of Personal data by Europol in Support of Criminal Investigations, and Europol's Role in Research and Innovation [2022] OJ L169/1 (Amended Europol Regulation); cf also Europol, 'Right of Access' (27 March 2024) <https://www.europol.europa.eu/right-of-access>.

723 According to Police Directive Art 2(1) in conjunction with ibid, Art 1(1), the directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It does not, however, apply to Union

Directive, entails a raft of actions such as storing, structuring, using or consulting data.[724] Therefore, when a law enforcement authority asks for or, at the latest, is granted access to personal data stored in Eurodac, the Police Directive is applicable. With regard to Europol, which is an EU Agency, the Data Protection Directive for EU Institutions and Bodies applies.[725]

The legal basis changes when law enforcement authorities access data recorded in Eurodac. This, it may be argued, triggers an additional obligation to provide information to the data subject. The identity of the controller also changes, or at least a second controller emerges in the context of joint controllers. As soon as data are processed under the Police Directive or the Data Protection Directive for EU Institutions and Bodies, Art. 42(1)(a) Eurodac Regulation requires that data subjects be informed about this change. Art. 13 Police Directive sets out a specific list of information that must be provided to data subjects,[726] and this applies as soon as data fall within the scope of the Directive. The same requirement applies when Europol accesses Eurodac data, which are then processed under the Data Protection Directive for EU Institutions and Bodies.[727]

However, Art. 18 Police Directive states that "Member States may provide for the exercise of the rights referred to in Art. 13, 14 and 16 [Police Directive] to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case

institutions, bodies, offices and agencies, such as Europol or Eurojust, according to ibid, Art 2(2)(b).

724 ibid, Art 3(2). Processing under the Police Directive means, according to Art. 3(2) any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Whether access, in case of law enforcement authorities accessing Eurodac, is already governed by the Police Directive is, however, unclear. There is no definition of the term access in the law and existing case law does not clarify the term either. Since "consulting" data is, however, already a form of processing, one might argue, that accessing data by law enforcement authorities already falls under the Police Directive.

725 Data Protection Regulation for EU Institutions and Bodies, Art 1(1); Europol Regulation; Amended Europol Regulation 2022; cf also Europol, 'Right of Access' (n 722).

726 Data subjects according to Police Directive, Art 6, are persons suspected of having committed a crime or to commit a crime, persons convicted of a criminal offence, victims or suspected victims and other parties to a criminal offence such as witnesses, contacts or associates of potential criminal offenders.

727 Data Protection Regulation for EU Institutions and Bodies, Art 14ff.

file processed in the course of criminal investigations and proceedings". This means that Member States may regulate the exercise of the right to information based on national law, at least in cases involving judicial procedures. Differences in national criminal procedures make it difficult to determine to what phase of a prosecution "criminal investigations and proceedings" refers.[728] Since the term 'processing' is defined broadly under the Police Directive and, pursuant to Art. 3(2), includes the 'consultation' of data, it can be argued that the right to be informed under Art. 13 Police Directive applies at the moment a request by law enforcement authorities to access Eurodac data is granted. Only later, when such data are incorporated into a judicial record, file, or decision, does Art. 18 of the Police Directive become applicable, and any diverging national law may then apply.[729] From

728 Mireille M Caruana states that, "[…] practical instances in which such national rules would apply are unclear, as the different national criminal procedural laws of the Member States make it difficult to determine what phase of a prosecution is referred to. It is also unclear whether the prefix 'judicial' in 'judicial decision' should also be taken to attach to 'record' or 'case file' (as in 'judicial record' or 'judicial case file'?)." She further suggests, that a reading of Recital 20 Police Directive suggests that: "This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings." Mireille M Caruana, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33 International Review of Law, Computers & Technology 257; Juraj Sajfert and Teresa Quintel only state that Police Directive Art 18 "means that the Directive is fully applicable to criminal proceedings" Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' [2017]; Mark Cole and Franziska Boehm, *Commentary on the General Data Protection Regulation* (Edward Elgar 2018) 7; The Working Party understands the proposed Article 17 (and recital 82) (equivalent to Police Directive, Art 18 (and Recital 107) later adopted) to mean that "Member States can decide to not align their national rules on criminal procedure with the rights as provided under Articles 11-16, at least in those cases where judicial procedures are concerned. [..]. The Working Party invites the European legislator to ensure no doubt can exist that the Directive applies to criminal procedures and the prosecution of crimes, also to avoid situations that no data protection would be offered as soon as a prosecutor or investigative judge is involved in a law enforcement operation or investigation, in line with Council of Europe Convention 108" (Art. 29 WP, 'Opinion 01/2012 on the Data Protection Reform Proposals' (2012) 00530/12/EN WP191 27).

729 The Art. 29 WP states that no doubt can exist that the "Directive applies to criminal procedures and the prosecution of crimes" and urges "to avoid situations that no data protection would be offered as soon as a prosecutor or investigative judge is

the foregoing, it can be concluded that individuals whose data have been collected under the Eurodac Regulation have a right to be informed when law enforcement authorities access their data.

This understanding of the right to be informed aligns with the case law of the CJEU concerning privacy and data protection laws. In 2016, the ECJ, drawing the Digital Rights Ireland judgment[730] and the invalidated Data Retention Directive,[731] defined in its ruling in Tele2 Sverige the conditions under which providers of electronic communications services must grant competent national authorities access to retained data. It held that "the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities".[732] Data stored in Eurodac may be regarded as 'retained data' within the meaning of these judgments. Such data are collected and stored for five to ten years from individuals who, at the time of collection, in most cases have no known connection to any criminal investigation.[733] Interoperability systems, too, have been considered "a new variation of data retention", since they will massively use data of individuals who are neither related to any crime

involved in a law enforcement operation or investigation, in line with Art. 29 WP, 'Opinion 01/2012 on the Data Protection Reform Proposals' (n 728) 27.

730 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] OJ C 175/6.

731 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).

732 *Tele2 Sverige* (n 522), para 121; In general, limitation to the right to information should not be interpreted too broadly since in *S and Marper v United Kingdom* [2008] ECHR 1581, paras 84 and 86, the ECtHR stated that already the retention of fingerprints by law enforcement authorities amounts to an interference with the right to respect for private life.

733 One could argue that asylum seekers and especially migrants that did not ask for asylum but also irregularly crossed a border or are irregularly present in the Schengen area, already committed a criminal offence by crossing a border irregularly, which is illegal in most Schengen states. However, such a minor offence mainly stipulated in administrative laws (immigration laws) and not criminal codes, should not be sufficient to exclude them from the application of the case law on data retention.

nor travelling with a false or more than one identity.[734] Therefore, storage of data in the (interoperable) Eurodac is comparable to the retention of personal data from users of electronic devices.[735]

It should be added that the CJEU also found that access to retained data by competent national authorities requires prior authorisation by either a court or an independent authority.[736] This requirement for the establishment of data retention schemes is recurring in the Court's judgments, which is why Quintel has suggested that this should be regarded as a general principle.[737] No such authorisation is necessary when national

734 Hartmut, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (n 73) 104; also, in M. K. v France, the ECtHR concluded that retention of fingerprints solely for the reason of preventing future identity theft would, in practice, be tantamount to justifying the storage of information on the entire population, which is clearly excessive (*M. K. v France*, App no 76100/13 (ECtHR, 1 September 2015) para 40).

735 It is worth mentioning here, that the ECJ foresees much stricter rules, when it comes to access by law enforcement authorities to retained data than the Eurodac Regulation does. It states in judgment *Tele2 Sverige* (n 522), para 119: In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, *only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime* (cf also, by analogy: *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 12 April 2015), para 260). However, in particular in situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities." And para 120: "In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (cf by analogy, in relation to the Data Retention Directive *Digital Rights Ireland Ltd v Minister for Communications and Others* (n 730) para 62; see also, by analogy, in relation to Article 9 of the ECHR, *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 6 June 2016))."

736 cf e.g., *Tele2 Sverige* (n 522), para 120.

737 Teresa Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (n 71) 11; even the CJEU states in: *Tele2 Sverige* (n 522), para 120, that "[i]n order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body …".

law enforcement authorities access data in Eurodac. Only the processing of information obtained by Europol through comparison with Eurodac data requires authorisation. Such authorisation must be obtained via the Europol national unit of the Member State of origin[738], which is not a court. It is therefore debatable whether a Europol unit can truly be regarded as independent in this context.

In another case before the ECJ, Bara et al.,[739] the Court addressed general administrative authorities rather than law enforcement authorities. The Court emphasised that the requirement to inform data subjects about the processing of their personal data is essential. This requirement creates the necessary conditions for data subjects to exercise their rights of access and rectification concerning the processed data. Additionally, it enables them to object to the processing of their data.[740] Consequently, the requirement of processing personal data in good faith[741] obliges an administrative authority to inform the data subjects that their personal data will be transferred to another administrative authority to be processed by it in its capacity as their recipient.[742] Also, information in relation to further processing must be provided "prior to that further processing".[743] National migration authorities processing Eurodac data should, therefore, inform the data subject once access has been granted to law enforcement authorities.

Based on the foregoing analysis, it can be concluded that data subjects whose data are stored in the Eurodac information system should first be informed in advance – prior to the collection of their fingerprints and facial images – about the potential use of their data by other recipients. They should then be notified again when their data have been accessed by law enforcement authorities, at the latest once such notification can no longer jeopardise an ongoing investigation. In cases where data are transferred to a third country following a law enforcement hit, the data subject should be informed before the transfer occurs. This approach ensures compliance

738 Eurodac Regulation 2024, Art 34(4).
739 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* (n 552).
740 ibid, para 33.
741 Provided for in Data Protection Directive 95/46/EC, Art 6 (no longer in force, date of end of validity: 24/05/2018; repealed by GDPR); now under GDPR, Art 5.
742 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* (n 552), para 34.
743 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 24 para 48.

with the requirement that the transfer does not create a real risk of violating fundamental rights.[744]

bbb) *Interoperability Regulation*

Art. 47 Interoperability Regulation provides that "the authority shall provide the information at the time that such data are collected." This may be interpreted in the same manner as the wording in the Eurodac Regulation or the GDPR: information should be provided before the data subject submits their personal data.[745]

As mentioned above, some interoperability systems can be considered a variation of data retention, as they will massively store and use data of individuals who are neither related to any crime nor travelling with a false or more than one identity.[746] The competent national authorities to whom access to the (retained) data has been granted must therefore notify the data subject as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.[747] The Interoperability Regulation provides a specific right to be informed about a red link, as long as no limitations to this right are necessary to protect security and public order, prevent crime, and guarantee that no national investigation will be jeopardised.[748] Based on the CJEU case law mentioned above, data subjects must be informed about the red flag at the latest after the reason for the restriction of the right to information has ceased to exist.

Apart from the red flag, no explicit right to be informed exists. If, following an examination of data sets indicating a false identity, data stored in the MID are found to be factually inaccurate or unlawfully recorded, the responsible Member State – or, where applicable, the requested Member State – must correct or delete the data, without any obligation to inform the individual of the correction.[749] While the case law mentioned above does not directly address this situation, it can nonetheless be argued, in

744 Eurodac Regulation 2024, Art 50(1).
745 cf above section: Informed When?
746 Hartmut, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (n 73) 1014.
747 *Tele2 Sverige* (n 522), para 121.
748 Interoperability Regulation - Judicial Cooperation, Art 32(4).
749 ibid, Art 47(4); FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 52.

light of the principle of transparency, that the data subject has a right to be informed in such circumstances.

VIS and ETIAS carry out comparisons of data with Eurodac.[750] ETIAS National Units can consult Eurodac for the purpose of examining applications for travel authorisation. They consult Eurodac in a read-only format. Following consultation, the result of the assessment is recorded only in the ETIAS application files.[751] Visa authorities can consult Eurodac in a read-only format for the purpose of manually verifying hits triggered by the automated queries carried out by the VIS[752] as well as examining and deciding on visa applications.[753,754] If it becomes clear during a visa procedure that a data subject has already sought asylum in a Member State before applying for a visa, it must be assumed that they will not be granted a visa (due to the risk that they would not leave the state). The question arises as to whether an individual has a right to be informed of a Eurodac hit in the context of a visa or travel authorisation procedure. Based on the principle of transparency and the aforementioned case law, which establishes a right to information when data are transferred between authorities, it is argued here that the data subject does indeed have a right to be informed.

In any case, data subjects may have to be informed whenever the interoperability system is expanded or modified in any way, in accordance with Art. 13(3) GDPR. The further processing of stored data for purposes other than those for which they were originally collected, or granting access to new recipients without notifying the data subject, would render such actions unlawful.[755] As noted above, this position is contested whenever new purposes are grounded in Union law. It is likely that interoperability will continue to evolve in the years following its implementation. How the millions of individuals whose data are stored in the information systems

750 Amendment to the VIS Regulation 2021, Art 9(a); ETIAS Regulation, Art 11.

751 Eurodac Regulation 2024, Art 8(b).

752 Amendment to the VIS Regulation 2021, Art 9(a) and 9(c).

753 According to the Visa Code, Art 21.

754 Eurodac Regulation 2024, Art 8(c).

755 Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602) 430; Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 53ff; Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 16 para 29; cf also *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* (n 552); Furthermore, data subjects have to be informed in case of a data breach: Art. 29 WP, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (2019) 18/EN WP250 rev.01.

linked through interoperability will be meaningfully informed remains a significant and open question.

c) *Informed How?*

aa) The Leaflets

As discussed above, the right to information under the Eurodac and Interoperability Regulations includes a range of information that must be offered to data subjects when they provide their biometric data to Eurodac. To this end, the EU produces leaflets containing information about Eurodac and the objectives of the AMMR, as outlined in Art. 19(1).[756] These leaflets already exist with regard to the Eurodac Regulation 603/2013 and the Dublin procedure. As of now, there are four different versions of this leaflet. The first contains two parts and is addressed to applicants for international protection.[757] The second part specifically addresses applicants in a Dublin procedure.[758] The second leaflet is for asylum seekers who are minors,[759] the third for third-country nationals or stateless persons apprehended in connection with the irregular crossing of an external border,[760] and the fourth for persons found irregularly staying in a Member State.[761] Member States using these leaflets are supposed to translate them into the corresponding languages and add information regarding their national asylum system.[762]

Information has to be provided in an "intelligible" way, according to the Eurodac Regulation, which means that it should be understood by an average member of the intended audience.[763] The language should be short and

756 Eurodac Regulation 2024, Art 42(1)(a).
757 Commission Implementing Regulation (EU) No 118/2014 of 30 January 2014 Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Asylum Application Lodged in One of the Member States by a Third-Country National [2014] OJ L39/1 (Dublin III Implementing Regulation).
758 ibid, Amendment X, Part B.
759 ibid, Amendment XI.
760 ibid, Amendment XII.
761 ibid, Amendment XII.
762 Dublin III Regulation, Art 4(1), (3); Eurodac Regulation 2024, Art 42(3).
763 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 7 para 9.

direct, avoiding complicated legal constructions.[764] The data subject should be able to determine in advance what the scope and consequences of the processing entail.[765] Information should furthermore be structured so as not to overwhelm the data subject, thereby avoiding so-called information fatigue.[766] Additionally, information has to be provided in a language the data subject understands or is "reasonably supposed to understand".[767]

All four versions of the information leaflets provide relatively detailed information and most of the information listed in Art. 29 Eurodac Regulation 603/2013. However, for the average asylum seeker, it will most likely not be clear that the first Member State which took fingerprints is primarily responsible for the asylum application. Part A of the leaflet for asylum seekers states that "[t]he country that will examine your request is determined through a process established by a European Union law known as the "Dublin" Regulation". It continues, that "[t]he law sets out various reasons why a country may be responsible for examining your request". The leaflet names "whether you have travelled to, or through, another Dublin country, either legally or irregularly" as such reasons. Towards the end of the leaflet, it is stated that "[y]our fingerprints will be checked within Eurodac to see if you have ever applied for asylum before or to see if you were previously fingerprinted at a border. This helps to determine which Dublin country is responsible for the examination of your asylum request". As an average person who first applies for asylum, this does not clearly convey that fingerprints are the primary factor in determining the Member State responsible for the application nor that travelling without authorisation may result in being returned to that state.

Only in Part B of the leaflet, intended for applicants subject to a Dublin procedure, is it indicated that if "your fingerprints were taken in another Dublin country (and stored in a European database called Eurodac)," that country may be responsible for the application. The same applies to the fact that people may be sent back to the Member State where they first provided their fingerprints.[768]

764 Zanfir-Fortuna, 'Article 5 - Principles relating to processing of personal data' (n 602) para 427.

765 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 7 para 10.

766 ibid 19, para 35.

767 Eurodac Regulation 2024, Art 42(1).

768 Part B of the leaflet states: "You are not supposed to move to another Dublin country. If you move to another Dublin country, you will be transferred back here or to a

In practice, this means that, at present, asylum seekers can only understand the significance of Eurodac once they are already subject to a procedure to be transferred to another Member State, rather than at the time their fingerprints are collected.[769] This is despite the fact that data subjects should be able to ascertain in advance the scope and consequences of the processing.[770] The CJEU has, however, ruled that third-country nationals staying irregularly in a Member State must be provided with both Part A and Part B of the leaflet.[771] It is hoped that future versions of these leaflets will clearly include the consequences and functions of biometric data processing in all sections.

It is rather vaguely indicated that all migration and police authorities within the Schengen Area (with certain exceptions for Schengen/Dublin-associated countries) may have access to the data.[772] Data subjects should understand that their data will be checked against Eurodac records by each Member State they enter and may be accessed by law enforcement authorities across Europe.

The incompleteness or vagueness of the leaflets may appear to be a rather theoretical problem. Conveying the information in practice, as will be described below, is the much bigger challenge. Within the overall structure of the European migration system, however, this vagueness and lack of transparency are systematic, serving a policy of deterrence and isolation, as this study will demonstrate. In their current form, the leaflets provide no information regarding interoperability, as Eurodac is not yet interoperable. It will be important to observe how information about interoperability is conveyed in the future. Once interoperability becomes operational, such vagueness and lack of transparency may leave asylum seekers or irregular migrants with little or no understanding of how their data are being processed.

---

country where you previously asked for asylum. Abandoning your application here will not change the responsible country. If you hide or run away, you also risk being detained."

769 as required in *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), para 87.

770 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 7 para 10.

771 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), para 90.

772 The leaflets state: "As of 20 July 2015, your fingerprints may be searched by authorities such as the police and the European police office (Europol) who may request access to the Eurodac database for the purpose of preventing, detecting and investigating serious crimes and terrorism."

bb) Receiving Information on the Ground

It is difficult to verify what information migrants actually receive when they are apprehended by the police or border guards or when they apply for international protection. The EU provides, as discussed above, leaflets with information. The question remains whether these leaflets or the information on them respectively reaches the data subjects. Several studies show that in the past, many data subjects had only fragmentary or even false knowledge about what their data were registered for.

One report shining light on this question was compiled in 2019 by Eurodac SCG.[773] The study was conducted in the aftermath of the latest revision of the Eurodac Regulation, which came into force in 2015.[774] For this, the Eurodac SCG drafted a questionnaire, which was sent to EU Member States in 2017.[775] Accordingly, the results show what Member States have reported themselves. With regard to the right to information, the study does not distinguish between different kinds of data subjects (e.g., asylum seekers, migrants apprehended during the crossing of an external Schengen border etc.).

To provide information, "the majority" of Member States reported using the model leaflets drafted by the EU, while others have developed their own informational materials.[776] While some countries provide the leaflets in different languages, several rely on oral translation with the help of a translator, expecting the data subjects to retain the information verbally.[777] Although most Member States distribute the leaflets, one reported merely showing the leaflet to the data subject, while another only provides the information via a website.[778] The majority of the Member States do not have a specific website or part of a website to inform data subjects about their rights.[779]

773 Eurodac SCG, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (n 694). A similar report was already done in 2009 and the results were similar. It seems, the practice regarding information has not evolved much over the years (cf Secretariat of the Eurodac Supervision Coordination Group, 'Eurodac Supervision Coordination Group: Second Inspection Report' (2009)).

774 Eurodac SCG, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (n 694) 2.

775 ibid 2.

776 ibid 6, Q6.

777 ibid 6, Q6.

778 ibid 7, Q8.

779 ibid 8, Q9.

According to the study, "a majority" of Member States document that information has been given to data subjects by letting them (and in some cases also a staff member) sign a written document. In some States, this is kept in the application file.[780] The study also states that "a considerable number" of Member States check whether the received information was understood by asking the data subjects orally. Some assume this by the signature in writing.[781]

The study lacks substantial detail, but the fact that several Member States openly admit in a self-declaration that they provide information only orally and do not verify whether data subjects have understood it, is quite revealing. Consequently, it seems fair to assume that the right to be informed is being violated for a large number of data subjects in Europe. This assumption is confirmed by another study conducted by FRA and published in 2018.[782] The study was conducted with legal and deskwork as well as fieldwork in six EU Member States.[783]

The study concluded that Member States rely predominantly on written information to fulfil their duty to inform asylum applicants along with other migrants whose fingerprints are taken and stored in Eurodac. Other than the Eurodac SCG study, the FRA study notes that most Member States have information on Eurodac available on a website.[784] It finds that, in the six countries studied, the EU-provided leaflets are available in the most commonly spoken languages by asylum seekers, and that authorities often obtain proof of confirmation that the information was provided.[785]

However, the study also shows that many migrants and applicants for international protection were unaware of the reasons why they had to provide their fingerprints. They knew even less about what would happen to their data.[786] Migrants stated that they have not been given information as to why their fingerprints were taken, where they were stored, and generally did not remember receiving information on their rights to access, correct, and delete their data.[787]

780 ibid 5, Q2.
781 ibid 5, Q3.
782 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70).
783 ibid 27, 31.
784 ibid 32.
785 ibid.
786 ibid 33.
787 ibid.

Several people interviewed who had transited to other Member States mentioned that they had received contradictory information from the Hungarian authorities. Some were told the fingerprinting was for security reasons and that they could be deprived of their liberty if they did not oblige. Others were told the fingerprinting would not affect which country had to process their application.[788] Migrants reported misleading, incomplete, or even no information at all from other countries, like Germany, Greece, the Netherlands, Spain, or Italy.[789]

The study states that officials in Germany and Sweden admitted that information given to migrants is often not understood correctly, if at all. In Italy, the field study concluded that information is often not provided in a manner that allows migrants to comprehend the implications of the fingerprinting.[790] "I don't think I have ever met an asylum seeker who knew what happened or why it happened. [...] Or what happens to them [the fingerprints]. Many of them ask, "How long are they kept, the fingerprints? Who can see them? My employer – can they see from the fingerprints that I am an asylum seeker? You get many questions," said a provider of legal assistance from Sweden.[791]

FRA's study not only finds a lack of understanding and of adequate information provided; it was able to make out some factors that influence how information is received. The study shows that language and the trustworthiness of the provider of information play a crucial role in how information is perceived and believed.[792] An earlier study by FRA also shows that levels of trust in the source providing information and communication barriers – due to both language and technical jargon – emerge as recurrent obstacles to effective provision of information.[793] Applicants for legal protection often consider friends, fellow compatriots, or other asylum seekers as a more trustworthy source than authorities.[794] The information received through

788 ibid.
789 ibid.
790 ibid 34.
791 ibid.
792 ibid.
793 ibid 33; FRA, 'Access to Justice in Europe: An Overview of Challenges and Opportunities' (n 205).
794 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70); there are also national studies supporting these finding, e.g., Associazione per gli Studi Giuridici sull'Immigrazione (ASGI), 'L'informativa Legale in Frontiera: Approccio Hotspot e Zone Di Transito Di Porti e Aeroporti' (2024) Analisi Giuridica.

these sources often turns out not to be accurate, leading, for example, one migrant to believe that giving fingerprints in Greece would not affect their future asylum case in another EU country.[795] FRA also finds that transparency about the purpose of data collection can encourage the data subjects to cooperate with the authorities.[796]

The study concludes that individuals lack awareness of data protection violations and available remedies, corroborating earlier FRA studies conducted since 2010.[797] Other research supports these findings. For instance, a study by the European Council on Refugees and Exiles (ECRE) revealed particularly concerning issues in border procedures: the right to be heard and the procedural guarantees outlined in the Asylum Procedures Directive are often not fully implemented. Key rights, including access to information, legal assistance, and interpretation, are either not provided or only partially enforced.[798] The Eurodac SCG, as early as 2009, already described the information on Eurodac as "more general and incomplete," noting that with respect to the "quality of the right to information, only a minority considered the information provided fully compliant with the Eurodac Regulation [...]".[799] A study by the EU Commission came to similar conclusions.[800]

It is important to note that individuals applying for international protection or migrants apprehended in irregular situations often face many serious concerns. As a result, their capacity to fully absorb and understand the information provided to them is limited. This is especially true when it comes to complex issues like data protection.[801] When information has to

795 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 34ff.

796 FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 46.

797 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 29 fn 48.

798 ECRE 'Border Procedures: Not a Panacea' (n 701) 3; Wagner and Katsiaficas, 'The State of Play of Schengen Governance: An Assessment of the Schengen Evaluation and Monitoring Mechanism in Its First Multiannual Programme' (n 701) 28; Asylum applicants also have the right to receive individualised legal and procedural information during the (border) procedure, unless they have access to free legal assistance.

799 'Eurodac SCG: Second Inspection Report' (n 773) 12.

800 DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (n 695) 8ff.

801 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 29.

be intelligible, i.e., it needs to be understood by the intended audience,[802] the circumstances in which data subjects have to absorb information have to be considered. The transparency principle requires that data subjects should not be taken by surprise regarding the purposes for which their personal data are processed.[803] Many of them will be. The failure to provide information, or the provision of misleading information, regarding the purpose of data processing is considered a breach of the transparency principle and, according to some authors, also of the fairness principle.[804] The fact that information only has to be provided in a language the data subjects are "reasonably supposed to understand"[805] may exacerbate the situation. It has been noted that this formulation carries serious risks that insufficient efforts will be made to ensure the applicant has effectively understood the information, thereby hindering their access to (international) protection.[806]

When an information system serves a number of purposes, data subjects have more issues understanding the information they receive.[807] This will definitely be the case when interoperability becomes operable.[808] It is evident that to guarantee the right to information, the asylum procedure, as well as the procedures for apprehending individuals crossing a border or staying irregularly in a Member State, would need to be revised.

802 Art. 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (n 568) 7 para 9.

803 ibid 23-24 para 45.

804 Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union* (Wolters Kluwer 2018) 121; Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (2nd edn, Oxford University Press 2004) 66.

805 Eurodac Regulation 2024, Art 42(1).

806 Vincent Chetail and Marian Ferolla Vallandro do Valle, 'The Asylum Procedure Regulation and the Erosion of Refugee's Rights' (*eumigrationlaw.blog.eu*, 23 May 2024) <https://eumigrationlawblog.eu/the-asylum-procedure-regulation-and-the-erosion-of-refugees-rights/>; ECRE, 'Information Note on Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on Common Procedures for Granting and Withdrawing International Protection (Recast)' (2014) 17ff.

807 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 9; FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 46.

808 According to the Activity report of the Eurodac SCG, the group discussed the findings of FRA and as a result the leaflets mentioned above, where drafted. The report refers to them as "tool" (Secretariat of the Eurodac Supervision Coordination Group, 'Eurodac SCG: Activity Report 2018-2019' (2020) 5).

cc) Children or Persons with Disabilities

aaa) *Children*

Reception systems for children vary greatly in Europe.[809] According to the Eurodac SCG study, "a great majority" of Member States have measures in place to inform minors in an age-appropriate way, whether through specific leaflets, brochures, staff members with specific training, or a legal guardian/social worker.[810] Some countries, for example, Switzerland, Germany, and Sweden,[811] provide leaflets with information especially for minors. In others, such as Belgium, there is a specialised unit responsible for relaying information to children in a way adapted to them through comic books or visual aids.[812] However, in practice, children are often not informed properly.

Children who arrive with their parents are regularly not informed separately, according to the above-mentioned FRA report.[813] Unaccompanied minors are often not informed in an understandable manner or at all.[814] Even worse, in several countries, the use of force to take fingerprints for Eurodac was reported, even for children and other vulnerable categories.[815]

809 cf e.g., IOM, UNHCR and UNICEF, 'Refugee and Migrant Children in Europe Accompanied, Unaccompanied and Separated: Overview of Trends (January to December 2020)' (2023); FRA, 'Mapping Child Protection Systems in the EU – Update 2023' (2024), chap 7.

810 Eurodac SCG, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (n 694) 6, Q5.

811 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 9; FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 46.

812 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 112.

813 ibid 38; cf also Stephanie Rap, 'Access to Justice and Child-Friendly Justice for Refugee and Migrant Children: International and European Legal Perspectives' [2020] Europe of Rights & Liberties/Europe des Droits & Libertés 277, chap 4.

814 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 9; FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 38, 45 and 111; cf also Rap, 'Access to Justice and Child-Friendly Justice for Refugee and Migrant Children: International and European Legal Perspectives' (n 813), chap 4.

815 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 9; FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 53: "First there is advice, then threats, then prolonged detention, then standing on a chair, maybe at night, in the office of the Scientific Police, then

Such practices have, to some degree, been legalised with Art. 14(1) Eurodac Regulation. This states that "where permitted by relevant Union or national law, and as a last resort, a proportionate degree of coercion may be used against minors to ensure their compliance with [the] obligation [to provide biometric data]." Such methods bear the risk of (re-)traumatising children[816] and make it impossible for them to understand what is happening.

Another problem is that children, especially unaccompanied minors, are sometimes treated as adults, therefore not receiving the treatment they would need in order for them to understand information they receive.[817]

Regarding the content of the leaflets or information given to children, it should be noted that the leaflets provided by the EU thus far do not provide any information on child trafficking and contact details of organisations specialised in this field that could be contacted by parents or children. This is the case even though many children go missing during the asylum procedure.[818] It is also worth noting that, according to Art. 14(3) Eurodac Regulation, even data pertaining to a child under the age of 14 can be used for law enforcement purposes. In many EU countries, this is the age at which a child is considered accountable under criminal law. Law enforcement access to data thus requires more than just "reasonable grounds".[819] Additional grounds are needed, unlike with minors above the age of 14 and adults.

---

forcing through pressure on the arm to put the hand on the machine collecting fingerprints." (Provider of legal assistance, male, Italy).

816 ibid 53.

817 ibid 108; see Ottavia Spaggiari, Isobel Thompson and Iliana Papangeli, 'How European Countries Wrongfully Classify Children Seeking Asylum as Adults' *The New Humanitarian* (10 April 2024) <https://www.thenewhumanitarian.org/investigations/2024/04/10/how-european-countries-wrongfully-classify-children-seeking-asylum-adults>; cf ECRE, 'Age Assessment in Europe: Applying European and International Legal Standards at All Stages of Age Assessment Procedures' (2023) Legal Note #13; cf also Council of Europe, 'Age Assessment for Children in Migration: A Human Rights-Based Approach' (2019) Ref. 139421GBR, 14.

818 cf Maria-Margarita Mentzelopoulou, 'Disappearance of Migrant Children in Europe' (European Parliament 2023): "In 2021, Lost in Europe, a journalism project investigating the disappearance of migrant children, reported that more than 18,000 migrant children had gone missing in Europe between 2018 and 2020."; 'Refugee and Migrant Children in Europe Accompanied, Unaccompanied and Separated: Overview of Trends (January to December 2020)' (n 809).

819 Eurodac Regulation 2024, Art 33(1)(d) and 34(1)(d).

Moreover, under the new Eurodac Regulation, children's data may be used for any purpose, including to assess whether they pose a security risk, even though the best interests of the child must be a 'primary consideration' for Member States when applying the Regulation.[820] This seems to imply that the best interest is not in every case *the* primary consideration but one among other "primary consideration[s]".

Since the Eurodac Regulation imposes virtually no restrictions on the use of children's data, it must be assumed that their data will also be used for interoperability purposes. This is concerning, given that children deserve specific protection regarding their personal data. They are less aware of the risks, consequences, and safeguards related to the processing of their personal information.[821] A child aged six or seven years will not be able to understand what data processing means, especially in such highly complex ways as in the interoperability systems.[822] Consequently, data processing within the interoperability systems should only be permissible if it is in the child's best interest. This means that children's data should, e.g., not be used for the purpose of detecting multiple identities.[823] The purpose of detecting multiple identities is absent from the Eurodac Regulation, even for adults. Regarding children, for whom the purposes of data processing should be more limited, such use of data appears impermissible. In any case, EU and national authorities must ensure that children – particularly those under the age of 14 –understand how their data will be used.

bbb) *Persons with Disabilities*

As seen above, neither Eurodac nor the Interoperability Regulation, nor the GDPR explicitly mention people with impairments in their provisions regarding the provision of information. With regard to the right to be informed, not all persons with disabilities are at a disadvantage and vul-

820 Eurodac Regulation 2024, Art 14(1).

821 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 83.

822 Bianca-Ioana Marcu, 'Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors' (*European Law Blog*, 29 April 2021) <https://europeanlawblog.eu/2021/04/29/eurodac-biometrics-facial-recognition-and-the-fundamental-rights-of-minors/>.

823 Interoperability Regulation - Judicial Cooperation, Art 25ff.

nerable.[824] Especially people with visual or hearing impairments, elderly persons, and persons with mental disabilities are at a risk of not receiving the information they need. Elderly persons are more likely to suffer from, for instance, visual and hearing impairments or are less used to modern technological systems. Only FRA's study considered this category of data subjects and found that they were not sufficiently informed.[825]

Children and persons with disabilities face an increased risk of having their right to information violated, and studies indicate that this often occurs in practice. The forthcoming interoperability of information systems is likely to exacerbate this problem. It is questionable whether such complex systems can be adequately explained to a child or to a person with cognitive impairments. This raises the further issue of whether it is even permissible to process data from these individuals within an interoperable information system. Excluding such data entirely would seem unfeasible, as it would remove children and persons with cognitive impairments from interoperability systems altogether. Nonetheless, this underscores a profound challenge in the operation of complex, datafied systems.

3. Consequences of a Violation: What Does This Right Do for Access to Justice?

The analysis above demonstrates that the right to information raises a number of unresolved issues, particularly concerning its scope and the timing of when information must be provided. It also highlights significant problems with the implementation of this right. Consequently, questions arise as to how data subjects can effectively exercise their right to information and what the implications are when this right is violated, especially in the context of asylum proceedings.

824 Clara Straimer, 'Vulnerable or Invisible? Asylum Seekers with Disabilities in Europe' (UNHCR Policy Development and Evaluation Service 2010) Research Paper No. 194, 8.

825 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 29ff and 101.

a) *Commentary and Scholars' Opinions*

A data controller who fails to provide a data subject with the information required by law, or provides it incompletely or incorrectly, breaches their legal obligation to inform. This obligation is set out in Art. 42 of the Eurodac Regulation and Art. 47 of the Interoperability Regulation, and its violation infringes the data subject's right to information. In this sense, the provision of information is a prerequisite for the lawful collection of data.[826]

The Eurodac Regulation contains only one provision, Art. 52, that regulates the consequences of unlawful data processing, stipulating a right to compensation for material or immaterial damage as a result of an unlawful processing operation. This liability provision will likely have little meaning in practice for data subjects. Not many will claim damages because their right to be informed was violated.[827]

The far more likely and frequent question in practice is: what happens if, as observed in the studies above, a data subject is not informed that their fingerprints are being used to determine the Member State responsible for their asylum application? For instance, what are the implications if they then travel irregularly to another country and apply for asylum there? Can they challenge the transfer decision back to the first country based on the breach of their right to information? Or, if a data subject has not been informed about who can access their data, can they claim that their data must not be accessed, e.g., by law enforcement authorities?

Bäcker argues that the failure to provide information has no legal consequences for the collection and further processing of data when it is based on Art. 6(1)(c) or (e) GDPR. This is because the data subject was obliged to disclose the data, regardless. In this case, it is argued, the obligation to provide information will merely have to be fulfilled at a later stage.[828] Only where the collection of data depends on the will of the data subject can a complete or partial omission of information undermine the formation of

826 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* (n 552), para 43; AG Yves Bot, 'Opinion 1/17 On the EU-Canada CETA Agreement' (Court of Justice of the European Union 2019); Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), no 8.162.

827 cf ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (2022) 87; see chapter: The Right to an Effective Remedy.

828 Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 65.

the will of the data subject. In this case, the breach of the duty to inform leads to the data collection being unlawful.[829] The further processing of the data is then, in principle, also unlawful, according to Art. 17(1)(d) GDPR.[830] Accordingly, the data must be deleted.[831]

If one follows this doctrine, the question arises as to what extent data subjects under the Eurodac Regulation have consented to the processing of their data. All of the data subjects under the Eurodac Regulation are obliged to provide their data, which is why it cannot be said that they provide their data voluntarily.[832] In theory, there is a debate as to whether asylum seekers have the option to choose the country in which they wish to claim asylum – a choice that is denied in practice.[833] Were such a choice available, the decision to provide personal data could be regarded as consent, as a data subject might argue that they would not have submitted their fingerprints to a Member State had they known it would assume responsibility for their asylum application; in practice, however, no such choice exists.

Dix, on the other hand, argues that this view fails to recognise the importance of the principle of transparency under the GDPR.[834] Transparency is

829 ibid, para 65.

830 ibid, para 67, 81.

831 ibid.

832 cf *Michael Schwarz v Stadt Bochum* (n 547), para 32: "[…] concerning the condition requiring the consent of persons applying for passports before their fingerprints can be taken, it should be noted that, as a general rule, it is essential for citizens of the Union to own a passport in order, for example, to travel to non-member countries and that that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004. Therefore, citizens of the Union wishing to make such journeys are not free to object to the processing of their fingerprints. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing."

833 cf Gamze Ovacık, 'The Right to Choose Country of Asylum: The 1951 Convention and the EU's Temporary Protection Directive' [2022] Forum on the EU Temporary Protection Responses to the Ukraine War <https://www.asileproject.eu/the-right-to-choose-country-of-asylum-the-1951-convention-and-the-eus-temporary-protection-directive/> accessed 17 April 2024; Violeta Moreno-Lax, 'The Legality of the "Safe Third Country" Notion Contested: Insights from the Law of Treaties', *Migration & Refugee Protection in the 21st Century: Legal Aspects* (Martinus Nijhoff 2015); cf also with regard to children and persons with disabilities, Alexander Dix, 'Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection regulation: Article-by-Article Commentary* (Nomos 2023), para. 2.

834 Alexander Dix, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019), para 26;

one of the fundamental conditions for lawful data processing. A violation of Art. 13 or 14 GDPR can, in his opinion, not be remedied by the subsequent provision of information.[835] The author also points to the fact that, for example, in Germany, it is not possible to fine a state authority.[836] In cases regarding Eurodac data, where in any case, state authorities have to provide the information, no legal consequences would therefore be possible.
If one takes this position, unlawfully collected data will have to be deleted even in cases where the data subject did not consent to the processing of data, which would include data subjects under the Eurodac Regulation.

b) *EU Case Law*

There is little case law in the field of the right to be informed. The ECJ has ruled on Art. 10 Directive 95/46/EC, which was replaced by Art. 13 GDPR, in the Bara et al. case in 2015, as mentioned.[837] This case concerned the transfer of data from one to another state authority and the question of whether the data subjects should have been informed about it. The Court recalled that the right to be informed may be restricted (under Art. 13 Directive 95/46/EC, and today under Art. 23 GDPR).[838] It regards the right to information as a prerequisite for the lawful collection and processing of data.[839]

In her opinion on the joined cases of five asylum seekers, Advocate General Kokott addressed the question of justiciability of the right to information. With regard to Art. 29 Eurodac Regulation 603/2013 (replaced by Art. 42 Eurodac Regulation), she stated that the right to receive the common leaflet is a right relating to the protection of data, not a procedural right in relation to the take-back procedure under the Dublin III Regu-

Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), no 15.

835 Dix, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 834), para 26; cf also Dix, 'Article 13 - Information to Be Provided Where Personal Data Are Collected from the Data Subject' (n 522), para 15.

836 GDPR 43(3); Dix 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 834), para 26.

837 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* (n 552).

838 ibid, para 39ff.

839 ibid, para 43.

lation.[840] "It is intended to promote the exercise of rights in connection with the protection of data, not to help improve the result of the transfer procedure. By extension, therefore, an infringement of that right cannot affect the outcome of the transfer procedure."[841] In essence, a violation of the right to information – pursuant to the Eurodac Regulation – may only influence the exercise of individual rights and has no bearing in the Dublin process (or in the future, the AMMR process), thus breaking the inextricable link between Eurodac and Dublin.[842]

However, Kokott later clarified that Art. 37 Eurodac Regulation 603/2013 (replaced by Art. 52 Eurodac Regulation) stipulates that affected individuals may seek compensation from the Member State responsible for any damages. This means that an infringement of Art. 29 Eurodac Regulation 603/2013 can be invoked, among other things, in the context of a challenge against a transfer decision.[843] She continued by stating that it seemed unlikely that a failure to provide the information set out in Art. 29 Eurodac Regulation 603/2013 would be such as to make it impossible to raise a consideration that would be relevant to the transfer decision.[844] If such a failure would make it impossible to raise a consideration to preclude a transfer and if this could not be remedied in the judicial procedure, it could lead to an annulment of the transfer decision.[845] In short, only if the failure to provide information deprives the data subject of presenting arguments that could have led to a different outcome of the administrative procedure, can the transfer decision be challenged based on the right to information.

840 Which is why the argument, made in EuGH, Case C-670/16 *Tsegezab Mengesteab v Bundesrepublik Deutschland* [2017] OJ C 309/17, para 48, cannot be made: "It follows from the foregoing: Case C-63/15 *Mehrdad Ghezelbash v Staatssecretaris van Veiligheid en Justitie* [2016] OJ C 296/12, that that provision (Dublin III Regulation, Art 27) must be interpreted as ensuring that the applicant for international protection has effective judicial protection by, inter alia, guaranteeing him the opportunity of bringing an action against a transfer decision made in respect of him, which may concern the examination of the application of that regulation, including respect of the procedural guarantees laid down in that regulation (cf to that effect Case C-155/15 *George Karim v Migrationsverket* [2016] OJ C 296/14, para 22)".

841 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 705), Opinion of AG Kokott, para 118.

842 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 408.

843 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 705), Opinion of AG Kokott, para 119.

844 ibid, para 120.

845 ibid, para 121.

This opinion was later confirmed by the ECJ in its decision in the same case.[846]

c) *National Case Law*

This study did not find many cases at the national level regarding the right to information. This may have something to do with the fact that data subjects' claims that they have not been informed are often not assessed by authorities and courts. As the studies analysed above show, many data subjects say that they received incorrect or insufficient information. In asylum, return or transfer procedures, such claims are sometimes not raised by the data subjects or their legal representatives. More often – according to countless conversations with legal representatives in Europe – the claims are not heard, investigated, or assessed by the courts or authorities. A legal counsellor in Switzerland, for example, states that she regularly raises the fact that asylum seekers in Croatia hardly receive any information about the Dublin process and even less about the Eurodac system – but she has never received a decision on this.[847] In practice, this means that the right to information is in many cases not justiciable.

Nevertheless, in France, a court ruled that a woman's right to information under the Eurodac and Dublin II Regulation had been infringed.[848] The woman was assisted in her asylum procedure by an association to which the French Office of Immigration and Integration had entrusted the implementation of initial reception actions but claimed that she did not receive the information provided by law. The court decided that the intervention of the association alone does not ensure the right to information, particularly on an individual's rights to access, rectify and appeal data.[849]

In another case in France, a court overturned the decision on a Dublin transfer of an asylum applicant to Spain by the Prefect of the Paris Police (*Préfet de police*), because the asylum applicant was not informed of essential safeguards, such as the use of his fingerprints, the identity of the

846 ibid, para 128.
847 This information was provided orally to the author by a legal counsellor working for Asylex.
848 Cour administrative d'appel de Nantes, 12 juillet 2011, 10NT02532, Juris-Data No. 2011-018043.
849 ibid.

data controller, and the recipients of the data.[850] However, in a later case in France, an asylum applicant sought annulment of their transfer under Dublin rules due to the failure of the French administration to provide them with relevant information in accordance with Art. 29 Eurodac Regulation 603/2013 and Art. 4 Dublin III Regulation. The Council of State (*Conseil d'État*) highlighted that the right to information is important for the protection of the applicant's personal data in the exercise of the rights of rectification or erasure. The court also held that such irregularities cannot result in a transfer decision being annulled.[851] Furthermore, according to the Administrative Tribunal of Nantes (*Tribunal administratif*) – in its decision of May 22, 2014 – that result could only be achieved when a breach of the right to information was coupled with concerns as to the deteriorated reception conditions (*in casu* in Italy), as a result of the increase of arrivals. In this case, the Italian authorities had not responded to the transfer request.[852]

In an Italian case, asylum applicants from Algeria and Pakistan sought to annul the decisions regarding their Dublin transfers to France, arguing that national authorities failed to provide specific information about the Dublin procedure. The Supreme Court of Cassation (*Corte Suprema di Cassazione*) clarified that the information required under Art. 4 and 5 Dublin III Regulation must be distinct from the information provided for the international protection procedure. The court reiterated the purpose and content of the obligations related to providing information as stated by the ECJ.[853] As a result, the court concluded that the decisions on the Dublin transfers should be annulled due to the breach of these obligations.[854]

---

850 Cour administrative d'appel, Jugement du 31 juillet 2014, No. 14PA00421; FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 29; another French court furthermore confirmed that a transfer decision must contain information on the remedies available, including the right to apply for suspensive effect, and the time limits for exercising these remedies and for the implementation of the transfer: Antoine Guérin, 'Décision de transfert Dublin anticipée: la CJUE souligne le détournement de procédure des préfectures françaises' [2018] La Revue des droits de l'homme; Case C-647/16 *Adil Hassan v Préfet du Pas-de-Calais* [2018] OJ C 259/9, para 71.

851 Conseil d'État, 7ème - 2ème chambres réunies, du 10 mai 2017, 406122.

852 *Tribunal Administratif de Nantes, Jugement du 22 juin 2012, N° 1505089.*

853 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714).

854 Corte Supreme di Cassazione - sezione civile, 3 aprile 2024, R.G. 10331/2024 (*Ricorrente / Ministero dell'Interno*).

In another case in France, the Administrative Court of Appeal of Lyon (*Cour administrative d'appel*) was confronted with an Afghan national who submitted an asylum claim in France but whose fingerprints were recorded in Slovakia, Sweden, and Italy in previous years. It held, in this context, that brochures were given to the applicant during the individual interview. According to the Court, the failure to provide the information to the applicant at the time he was informed of the date and time of his asylum application registration appointment did not deprive him of his right to information. Consequently, he was not entitled to argue that the decision ordering his surrender to the Italian authorities infringes Art. 4 Dublin III Regulation and the guarantees of the right of asylum.[855]

4. Conclusions

The examination of the right to information under the Eurodac and Interoperability Regulations reveals substantial challenges and inconsistencies in its practical implementation, affecting data subjects' access to justice.

The Eurodac Regulation lacks some clarity in what specific information must be provided regarding the purposes of data use, security flags, recipients, and data transfers to third countries. The Interoperability Regulation further complicates this landscape, introducing new systems and automated processing that require detailed and comprehensible communication to data subjects.

Ensuring timely information provision is crucial for transparency and fairness. Field studies indicate significant inconsistencies across Member States, with some failing to meet the required standards. Data subjects often receive information too late and/or not in a manner that ensures they comprehend it. This undermines their ability to understand and exercise their rights effectively.

855 Cour administrative d'appel de LYON (CAA de Lyon), 2ème chambre - formation à 3, 20 novembre 2018, 18LY01453, inédit au recueil Lebon: "En deuxième lieu, ces brochures ont été remises à M. A. lors de l'entretien individuel qui s'est déroulé le 28 octobre 2017, soit en temps utile pour faire valoir ses observations. La circonstance que ces documents ne lui auraient pas été remis dès le moment où la date et l'heure du rendez-vous fixé pour l'enregistrement de sa demande d'asile lui ont été communiqués n'a pas privé le requérant d'une garantie. Par suite, M. A. n'est pas fondé à soutenir que la décision ordonnant sa remise aux autorités italiennes méconnaît l'article 4 du règlement n° 604/2013 et les garanties du droit d'asile."

In addition, the methods used to inform data subjects, such as leaflets, often fail to convey critical details effectively. Vulnerable groups, like children and persons with disabilities, face additional barriers. The information provided is frequently not tailored to their needs. The complexity of interoperability systems further exacerbates these issues, making it imperative to enhance communication strategies.

Legal commentary and case law underscore the importance of the right to information as a prerequisite for lawful data processing. However, not only is the enforcement of this right inconsistent, there are significant gaps in judicial responses. National case law shows varied outcomes, with some courts recognising the impact of inadequate information provision. Others do not see it as sufficient to invalidate administrative decisions unless coupled with other procedural issues.

The failure to provide adequate information has profound implications for access to justice, particularly in asylum proceedings. Data subjects' inability to challenge decisions, such as transfer decisions, effectively based on a violation of their right to information undermines their right to access justice. Although legal provisions exist for compensation, their practical impact is limited, as many data subjects are unlikely to claim damages for informational rights violations alone.

Overall, the right to information, while enshrined in the Eurodac and Interoperability Regulations, faces significant practical challenges that impede its effectiveness in safeguarding data subjects' rights. Addressing these challenges requires a concerted effort to enhance transparency, ensure timely and accurate information provision, as well as recognise the substantive impact of informational rights on access to justice. Only through such measures can the right to information fulfil its intended role in the broader context of data protection and legal fairness.

II. The Right to Access Personal Data and Information

1. What Is the Right to Access Personal Data and Information?

The right of access to personal data is closely linked to the right to information.[856] The Eurodac and Interoperability Regulations address these two rights separately. While the right to information is designed as an obligation by the state to provide information without the data subjects having to ask for it, the right of access has to be exercised by the data subject itself.

The right of access to personal data is also closely linked to the rights to rectification and erasure of personal data: without access, it is practically impossible to know whether data stored about oneself is accurate.[857] In the Eurodac Regulation, these rights are contained in Art. 43; certain paragraphs deal only with the right of access and others only with the right to rectification and erasure. Because certain questions are particularly relevant in the context of access, and because of its links to the right to be informed and the rights of rectification and erasure, the right of access is dealt with separately in this study.

The right to access under the Eurodac Regulation is not structured as a right to public information and documents but to personal data and certain kinds of information.[858] The same goes for the right of access under the Interoperability Regulations.[859] Neither the Eurodac nor the Interoperabili-

856 See chapter: The Right to Information.

857 Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E Rijkeboer* [2009] ECR I-03889, para 51; Case C-154/21 *RW v Österreichische Post AG* [2023] OJ C 71/7, para 37ff; Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553) para 10.

858 cf Gabriela Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, Oxford University Press 2020) 452.

859 Interoperability Regulation - Judicial Cooperation, Art 48; Interoperability Regulation - Borders, Art 48.

ty Regulations contain a right of access to public documents.[860] The right of access is designed, in both regulations, as individual rights of access to personal data or data related to the data subject.

a) *International Human Rights Law Applicable in Europe*

International human rights law instruments generally treat the right to access personal data as an element of the broader right to information embedded in privacy protections. Under the ECHR, this right is grounded in Art. 8, which safeguards respect for private and family life.[861] The Court ruled that the national law of the contracting countries must provide an effective and accessible procedure, enabling applicants to have access to any important information concerning them.[862] In relation to personal data held by security services, it has further found that barriers to access may amount to a violation of Art. 8 ECHR.[863] In some circumstances, however, access rights may be significantly curtailed.[864] The right to obtain one's data and file also forms part of the right to an effective remedy under Art. 13 ECHR.[865]

860 However, the right of access to public information is important in the context of Eurodac and interoperability. For example, cases might emerge where individuals or organisations request information on the algorithms used within the interoperability system (Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 08.66: "the CFR, Art 42, lays down the right of access to documents held by EU institutions, bodies, offices and agencies. Individuals cannot invoke this provision against public authorities in their Member State. Whether such a right exists at national level depends in the first place on national law. However, the case law of the ECtHR reveals a gradual acceptance of a right of access to information held by public authorities as part of the right to freedom of expression, as laid down in the ECHR, Art 10").

861 ECtHR, 'Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life' (2020); also: *Torsten Leander v Sweden* (n 523); *Gaskin v the United Kingdom* (n 524); *KH and Others v Slovakia* App no 32881/04 (ECtHR, 6 November 2009).

862 *Yonchev v Bulgaria* App no 12504/09 (ECtHR, 9 December 2017), paras 49 - 53.

863 E.g., *Haralambie v Romania* App no 21737/03 (ECtHR, 27 October 2009), para 96.

864 E.g., *Segerstedt-Wiberg and Others v Sweden* [2006] ECHR 2006-VII, para 91.

865 *Tagayeva and Others v Russia* App no 26562/07 and 6 other applications (ECtHR, 13 April 2017), para 627; The ECtHR stated that under ECHR, Art 13, a person needs to be able to challenge the data storage or to refute the truth of the information, including when it is stored for security purposes (*Rotaru v Romania* [2000] ECHR 2000-V, para 72).

Similarly, Art. 17 ICCPR, Art. 16 CRC and Art. 22 CRPD provide a right to privacy, which include the right to access personal data.[866] So does the non-binding Art. 12 UDHR. The UN states that processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access to data, among other things.[867] With regard to children, the Special Rapporteur on the Right to Privacy wrote that the "[s]tate and member bodies shall require the design and implementation of rights-based recordkeeping systems to support the human rights of all children, but particularly those in alternative care and forced migration environments, to provide agency to the child to access these records, and to enable accountability to the child for all deliberations and decisions impacting on the well-being of a child".[868] Concerning persons with disabilities, the UN recommends that states adopt guidance materials and protocols on the respect and protection of privacy and access to personal information. These are inclusive of persons with disabilities, targeting staff of public and private services, and institutions keeping records of personal data on persons with disabilities.[869]

Finally, Art. 8(b) of Convention 108[870] and Art. 9(b) of the Modernised Convention 108+,[871] also hold the right to access personal data. Art. 9(b) Modernised Convention 108+ states that "every person should be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him [or her] are stored in the automated data file as well as communication to him [or her] of such data in an intelligible form". According to the Explanatory Report, this wording is meant to accommodate the diverse approaches found in

866 cf regarding the ICCPR: Paul M Taylor, 'Article 17: Privacy, Home, Correspondence; Honour and Reputation', *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights* (Cambridge University Press 2020); regarding the CRC: Cannataci, 'Special Rapporteur on the Right to Privacy' (n 531); and regarding the CPRD: UN, 'Article 22: List of Illustrative Indicators on Respect for Privacy' (OHCHR 2020) Advance Version.

867 cf UN, 'Personal Data Protection and Privacy Principles - Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting' (2018).

868 Cannataci, 'Special Rapporteur on the Right to Privacy' (n 531).

869 UN, 'List of Illustrative Indicators on Respect for Privacy' (n 866).

870 Convention 108.

871 Modernised Convention 108+.

national laws: communication at the request of the data subject or at the initiative of the controller of the file; communication free of charge at fixed intervals, as well as communication against payment at any other time, etc.[872] The provision does not specify from whom the data subject should obtain communication. In most states, this will be the controller of the file; in some states, this right is exercised through the intermediary of the supervisory authority.[873] Exceptions and restrictions to these rights are contained in Art. 9 Convention 108 or Art. 11 Modernised Convention 108+, respectively.

b) *EU Human Rights Law: European Charter of Fundamental Rights*

The CFR provides in Art. 7 the respect for private and family life and in Art. 8 CFR the protection of personal data, explicitly granting access in paragraph 2 to "data which has been collected concerning him or her, and the right to have it rectified."[874] In its case law, the ECJ emphasises the significance of the right to access data. This may not be restricted by reference to the information duties, i.e., the right to information.[875] A person has a right to access their data, even when information about it has already been given to them – like in the case of asylum, transfer, or return proceedings, with regard to Eurodac data. Art. 52 CFR states the limitations on the right to access. The ECJ clarified, however, that national authorities must document why a restriction has been invoked, even in cases involving national security.[876] Some scholars have suggested that Art. 8(2) CFR must be interpreted using the proportionality test under Art. 42 CFR.[877] The right of access is necessary, inter alia, to enable the data subject to obtain,

872 Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (1981), no 53.

873 ibid, no 52.

874 For a more comprehensive analysis of these provisions see chapter: The Right to Information.

875 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857), para 68ff.

876 This was stated in the context of the Police Directive in Case C-333/22, *Ligue des droits humains ASBL, BA v Organe de contrôle de l'information policière* [2023] para. 70.

877 'Noyb Observations on EDPB Guidelines 01/2022 on Data Subject Rights – Rights of Access (n 556).

depending on the circumstances, the rectification, erasure, or blocking of their data.[878]

The right of access to data and one's own file is also part of the right to an effective remedy, as protected under Art. 47 CFR.[879] The right of access to documents is furthermore specifically protected under Art. 42 CFR and, the right to one's own file also by the right to good administration in Art. 41(2)(b) CFR.[880] Although Art. 41 reflects a general principle of EU law, the ECJ decided that Art. 41(2)(b) CFR could only be exercised against the institutions, bodies, offices, and agencies of the European Union.[881]

c) *EU Law: GDPR, Police Directive and Data Protection Directive for EU Institutions and Bodies*

aa) General Data Protection Regulation

Under the GDPR, the right of access by the data subject is contained in Art. 15. It is a concretisation of the fundamental right in Art. 8 CFR.[882] Art. 15 GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the

878 *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* (n 558), para 44; *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857) paras 49 and 51.

879 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559) para 47.119: "access to files will in reality often be a necessary pre-condition for successful litigation in the context of enforcing 'rights and freedoms guaranteed by the law of the Union'" with reference to, for example, Case C-536/11 *Bundeswettbewerbsbehörde v Donau Chemie AG, Donauchem GmbH and Others* [2013] OJ C 252/11).

880 cf e.g., Ivan Lazarov, 'Article 42 – Right of Access to Documents' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Bloomsbury Publishing 2022); Paul Craig, 'Article 41 - Right to Good Administration' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Publishing 2021); Tobias Lock, 'Charter of Fundamental Rights of the European Union - Article 41 and 42 CFR' in Manuel Kellerbauer, Jonathan Tomkin and Marcus Klamert (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (1st edn, Oxford University Press 2019).

881 *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), para 67ff.

882 Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553), para 2; cf Lynskey, 'Deconstructing Data Protection in the EU Legal Order: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (n 553); EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553).

Union, regardless of whether the processing takes place in the Union or not.[883] Data subjects outside of the EU have access rights, if their data are processed within the EU. There is, however, no provision regarding the procedure of such an extraterritorial request. The ECJ has delt with aspects of the extraterritorial application of the Directive 95/46, which has been replaced by the GDPR, in its case Schrems I.[884] Extraterritorial effects of the GDPR in non-EU, i.e., third countries, require the EU to ensure that the same level of protection, including access to judicial review, must exist in third countries to which personal data originating in the EU is transferred.[885]

Access to data can be asked from the controller, which is defined in Art. 4(7) GDPR, or any joint controller, irrespective of an agreement between the controllers as to who is to fulfil access claims.[886] The list of information and data accessible under Art. 15 GDPR overlaps with the information that must be provided to data subjects under Art. 13 and Art. 14, but data provided under Art. 15 must be much more precise and granular.[887]

The controller must provide the following information to the data subject: Whether personal data are being processed; the personal data itself; the purposes of the processing; the recipients or categories of recipients to whom the personal data have been or will be disclosed; the period for which the data will be stored, or the criteria used to determine that period; information about the existence of the right to request rectification or erasure of personal data from the controller; the right to lodge a complaint with a supervisory authority.[888] Additionally, data subjects can access information regarding the existence of automated decision-making, including profiling.[889] Whenever the personal data are not collected from the data

883 GDPR, Art 3; cf EDPB, 'Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)' (2019) Version 2.1.

884 *Schrems v Data Protection Commissioner* (n 175).

885 ibid, para 96; also: Opinion 1/15 On the Draft Canada-EU PNR Agreement (n 541), paras 322 - 327; Tobias Lock and Denis Martin, 'Charter of Fundamental Rights of the European Union - Article 47 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (1st edn, Oxford University Press 2019), para 20.

886 Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553), no 10.

887 Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 462.

888 GDPR, Art 15(1)(a) - (f).

889 ibid, Art 15(1)(h).

subject, any available information as to their source shall be provided.[890] If personal data are transferred to a third country or to an international organisation, data subjects have the right to be informed of the appropriate safeguards pursuant to Art. 46 GDPR relating to the transfer.[891] The controller has to provide a copy of the personal data undergoing processing.[892]

Restrictions to the access right apply according to Art. 15(4) GDPR, stating that "[t]he right to obtain a copy […] shall not adversely affect the rights and freedoms of others." Furthermore, Art. 12(5) GDPR states that the controller can refuse to act on the request if it is "manifestly unfounded or excessive, in particular because of their repetitive character." Finally, the general limitation in Art. 23 GDPR applies, i.e., the same restrictions as to the right to information in Art. 13 GDPR. They are based mainly on security concerns, the prevention or investigation of criminal offences, and other important objectives of general public interest of the Union or of a Member State. Some scholars also have suggested that a proportionality test should apply in order for the GDPR's provisions to provide more detailed results.[893]

bb) Police Directive

The Police Directive includes an access to data provision in Art. 14, which grants individuals access to several key pieces of information. This includes the purposes and legal basis for the processing, the categories of personal data involved, and the recipients of the data, including third countries or international organisations. Additionally, it specifies that, where possible, individuals should be informed about the period for which the data will be stored, as well as their rights to rectification or erasure. It also outlines the right to lodge a complaint with the supervisory authority and provides communication regarding the personal data undergoing processing, along with any available information regarding their origin.

Limitations under the Directive are specific to the right of access and contained in Art. 15. They refer to security issues, rights and freedoms of others, obstructing investigations or prejudicing the prevention, detection or investigation of criminal offences.

890 ibid, Art 15(1)(g).
891 ibid, Art 15(2).
892 ibid, Art 15(3).
893 'Noyb Observations on EDPB Guidelines 01/2022 on Data Subject Rights – Rights of Access (n 556).

cc) Data Protection Regulation for EU Institutions and Bodies

Art. 17 of the Data Protection Regulation for EU Institutions and Bodies also provides for the right of access to personal data, which largely overlaps with the right of access in the GDPR. Restrictions to this right apply according to Art. 25 Data Protection Regulation for EU Institutions and Bodies. They are based mainly on security concerns, the prevention or investigation of criminal offences, and other important objectives of general public interest of the Union or of a Member State.

d) *Eurodac Regulation*

The Eurodac Regulation contains a right to access to, rectification, and erasure of personal data in Art. 43. The right of access to personal data is specifically contained in Art. 43(1), (2), (3), (6), (7), (8) and (9) Eurodac Regulation. The right has to be exercised in accordance with Chapter III of the GDPR (Art. 12 ff.), which contains the rights of the data subjects.[894]

According to Art. 43(2) Eurodac Regulation the access right of the data subject in each Member State "shall include the right to have communicated to him or her the personal data relating to him or her recorded in Eurodac, including any record indicating that the person could pose a threat to internal security, and the Member State which transmitted them to Eurodac under the conditions set out in Regulation (EU) 2016/679 and in national law adopted pursuant thereto. Such access to personal data may be granted only by a Member State." Paragraph 3 holds that, with regard to a record indicating that the person could pose a threat to internal security, Member States may restrict the data subject's rights referred to in this article in accordance with Art. 23 GDPR. It is worth noting here that the Eurodac Regulation only states a right to access personal data and not to information. This would be much narrower than Art. 15 GDPR, which explicitly states that its access right grants "access to the personal data and the following information", followed by a list of information. The Interoperability Regulation, as we will see, refers to the GDPR with regard to its access right. However, the right to access personal data under Art. 43 Eurodac Regulation, and its predecessors, includes, at a minimum, the information that is provided to data subjects under Art. 42 Eurodac Regulation. This

894 Eurodac Regulation 2024, Art 43(1).

entails more than personal data, as for example the identity and contact details of the controller or the period for which data will be stored in Eurodac. The right to access personal data under the Eurodac Regulation therefore has to be understood, like the corresponding right in the GDPR, as a right to access personal and certain information.

The Eurodac Regulation stipulates that whenever a person requests access to data relating to them, the competent authority has to keep a record in the form of a written document that the request was made and how it was addressed. The authority has to make that document available to the national supervisory authorities without delay.[895]

The national supervisory authority of the Member State that transmitted the data and the national supervisory authority of the Member State in which the data subject is present have to, where requested, provide information to the data subject concerning the exercise of their right.[896] The supervisory authorities cooperate in accordance with Chapter VII of the GDPR, comprising provisions on cooperation and consistency.[897]

Eurodac stores data of data subjects located in a Member State but also of many that are not in one of the Member States (anymore). Data sets related to applicants for international protection are stored for ten years from the date biometric data are transmitted.[898] In contrast, data sets concerning other data subjects, in particular those apprehended irregularly crossing a border or staying in a Member State are stored in Eurodac for five years from the transmission date.[899] There are exceptions for certain groups: data subjects within Union resettlement frameworks who do not receive international protection or humanitarian status have their data recorded for three years,[900] while beneficiaries of temporary protection have their data stored for one year.[901] Data subjects, especially when they have left the Schengen Area, might have an interest in accessing their personal data. According to Art. 60 Eurodac Regulation, its provisions are not applicable to any territory to which the AMMR does not apply.[902] Whether this has an

895 Eurodac Regulation 2024, Art 43(8).
896 ibid, Art 43(9).
897 ibid.
898 ibid, Art 29(1).
899 ibid, Art 29(3), (5-8).
900 ibid, Art 29(4) in conjunction with ibid, Art 18(2)(b) or (c).
901 ibid, Art 29(9) in conjunction with ibid, Art 26(1).
902 The AMMR applies to 'Member States' and associated States. According to the AMMR, Art 66, [a]s far as the French Republic is concerned, the Regulation shall apply only to its European territory.

effect for data subjects outside the Schengen Area will be examined later in this chapter.

e) *Interoperability Regulation*

According to Art. 3, the Interoperability Regulations apply to individuals whose personal data may be processed in the EU information systems and in the Europol database. Unlike the Eurodac Regulation, the Interoperability Regulations can be applied extraterritorially. This means that if a data subject located outside the Schengen Area wishes to access data contained in one of the Interoperability systems, these regulations may be invoked.

The Interoperability Regulations hold in Art. 48 the right to access personal data stored in the MID. No access right is provided for data stored in the CIR or the sBMS. The Regulations refer to Art. 15 GDPR with regard to the right to access,[903] adding few additional procedural requirements. The Interoperability Regulations state a 45-day period, within which a data subject has to receive an answer,[904] after addressing themselves to the competent authority of a Member State to access their personal data.[905] The Regulations state the possibility to submit a request for rectification or erasure of data to another Member State than the one responsible for the verification of data.[906] They do not provide this for access and restriction requests.

Member States responsible for the manual verification of different identities, or the Member State to which the request has been made, must maintain written records of the access request. These records should be made available to the supervisory authorities without delay.[907]

903 Interoperability Regulation - Judicial Cooperation, Art 48(1) and (11); Interoperability Regulation - Borders, Art 48(1) and (11).

904 ibid, Art 48(2) states a period of 45 days, with a possible extension of another 15 days, in which an access request has to be examined. The Member State has to inform the data subject of such an extension within the 45 days period.

905 ibid, Art 48(1).

906 ibid, Art 48(3): "If a request for rectification or erasure of personal data is made to a Member State other than the Member State responsible for the manual verification of different identities, the Member State to which the request has been made has to contact the authorities of the Member State responsible for the manual verification of different identities within seven days. The Member State responsible for the manual verification has to respond within 30 days, with a possible extension of another 15 days."

907 ibid, Art 48(10).

A negative decision by a Member State has to provide the person concerned with all the relevant information as to how the decision can be challenged or how to bring an action or a complaint, and with information about assistance, including from the supervisory authorities.[908]

2. Scope and Limitations

a) *Who Can Access Data?*

aa) Data Subjects

The rights of access in Art. 43 Eurodac Regulation and Art. 48 Interoperability Regulation are individual rights. They apply to data subjects seeking access to their personal data in Eurodac or the MID. The overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data, so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.[909] This will make it easier – but is not a condition – for the individual to exercise other rights such as the right to erasure or rectification.[910] It should furthermore be noted that the ECJ confirms a right to obtain a copy of personal data, even where a request is motivated by a purpose other than those mentioned above.[911]

While the right to public information is often exercised by news organisations or non-governmental organisations (NGOs),[912] access to personal

908 ibid, Art 48(8).

909 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 2; cf also Eurodac Regulation 2024, Recital 82; Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553), para 1.

910 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 2 and 43 para 139; cf also *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857), para 51; *RW v Österreichische Post AG* (n 857), para 38; Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553), para 1; Matthias Bäcker, 'Artikel 15 - Auskunftsrecht der betroffenen Person' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020), para 10.

911 Case C-312/23 *Addiko Bank d.d. v Agencija za zaštitu osobnih podataka* [2024] para 2.

912 Although in *Magyar Helsinki Bizottság v Hungary* App no 18030/11 (ECtHR, 8 November 2016), para 156, the ECtHR considered that the time had come to clarify the classic principles on access to information under ECHR, Art 10, it considered

data is generally limited to the data subject. Anyone else must act on the individual's behalf or with their authorisation, for example through a power of attorney. Neither the Eurodac Regulation nor the Interoperability Regulation sets rules on legal representation, including how such authorisation must be demonstrated. Therefore, national law has to be taken into account in cases where someone wants to access personal data on someone else's behalf.[913]

bb) Children

aaa) *Use of Children's Data (Accompanied and Unaccompanied Minors)*

Eurodac stores data of children starting at the age of six.[914] While the initial Proposal for the Eurodac Regulation specified a narrow purpose for the use of young children's data – primarily to help establish their identity and assist a Member State in tracing any family connections or links with another Member State[915] – the new Eurodac Regulation allows for the use of children's data for broader purposes. This includes assessing whether they may pose a security risk. Additionally, children's data can be utilised for law enforcement purposes. The only restriction is that Eurodac data pertaining to a child under the age of 14 may be used for law enforcement purposes only if there are additional grounds – beyond those required for juveniles over 14 and adults[916] – to consider the data necessary for the prevention, detection, or investigation of a terrorist offence or another serious crime the child is suspected of having committed.[917] The Eurodac Regulation stipulates that the best interests of the child have to be "a

that the right of access was not necessarily restricted to public watchdogs but could be invoked by any individual in circumstances where the information is instrumental for the individual's exercise of her or his right to freedom of expression, in particular the freedom to receive an impart information, and where its denial constitutes an interference with that right.

913 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 27 para 80; Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 461.

914 Eurodac Regulation 2024, Art 14, 15, 18, 20, 22, 23, 24 and 26.

915 2016 Eurodac Proposal, Recital 25; cf also 2016 Eurodac Proposal, 'Explanatory Memorandum,' 9 and 13.

916 referred to in Eurodac Regulation 2024, Art 33(1)(d).

917 ibid, Art 14.

primary consideration" for Member States when applying the Regulation.[918] Whether the processing of children's data – particularly that of very young children – within an interoperable Eurodac system can ever be regarded as being in their best interests is open to doubt.[919] The wording of the Eurodac Regulation also implies that the best interest is not in every case *the* primary consideration but one among other "primary consideration[s]" – and the data collection and security interests of the Member States seem to be at the forefront.[920]

bbb) *Access to Children's Data*

Against the background of data protection considerations, it can be argued that data of persons that cannot fully comprehend and exercise their data rights (by themselves) should only be collected for narrow purposes and only if it serves these persons' best interests.[921] Therefore, the best interests of the child should be the leading consideration in all decisions taken with regard to children's data. This is particularly true where the right of access

---

918 ibid, Art 14(1).

919 cf FRA 'Age assessment and Fingerprinting of Children in Asylum Procedures' (2018); fn 921, 930.

920 Also, GDPR, Recital 71, states that automated decision-making should not concern a child, which seems to be in conflict with the use of children's data in the MID.

921 GDPR, Art 6(1)(f): "[…] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." According to Dix, 'Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services' (n 833), para 11, this means, the interests of a child must be given particular consideration when deciding whether or not the processing is in the legitimate interest of the data controller; cf also Recital 75 GDPR: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: … where personal data of vulnerable natural persons, in particular of children, are processed"; Also, according to Dix, 'Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services' (n 833), para 2, giving valid consent to the processing of personal data requires at least a general understanding of the consequences and risks associated with the permission and the rights that are available. Data subjects whose cognitive capabilities do not permit them to form a sufficiently accurate understanding of the content and the consequences of their consent do not consent freely.

is exercised on behalf of the child, for example by a parent.[922] It is necessary to examine the circumstances under which a child can independently request access and to what extent the holders of parental responsibility are permitted to make requests on behalf of the child.

According to the European Data Protection Board (EDPB) guidelines, children are data subjects in their own right. As such, the right of access belongs to the child.[923] Zanfir-Fortuna, too, argues that children should be allowed to ask for data access themselves.[924] Depending on the maturity and capacity of the child, the holder of the parental responsibility could be needed to act on the child's behalf.[925]

The right to access one's own data does not require legal capacity to act, such as entering into a contract.[926] The data subject does not create any obligations for themselves by submitting a request. They merely ask to receive information. In practice, whether children are allowed access will depend on the national legal systems of the Member State concerned and how legal competence in private law is regulated.[927] According to the European Commission, the age threshold for obtaining parental consent is established by each EU Member State and can be between 13 and 16

922 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 84.

923 GDPR, Recital 38 states that the EDPB has to produce a document to provide guidance on the conditions under which a child may exercise their own right of access, and the holder of parental responsibility can exercise the right of access on behalf of the child, which it did with the: EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 83ff.

924 Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 461.

925 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 84.

926 Dix, 'Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services' (n 833), para. 2: "Giving valid consent to the processing of personal data requires at least a general understanding of the consequences and risks associated with the permission and the rights that are available. Data subjects whose cognitive capabilities do not permit them to form a sufficiently accurate understanding of the content and the consequences of their consent do not consent freely."

927 cf Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 461; The EDPB suggests, that the right of the holder of parental responsibility to act on behalf of the child should not be confused with instances, outside of data protection law, where the national legislation may provide the right of the holder of parental responsibility to ask and receive information on the child (e. g. performance of the child at school) (EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 87).

years.[928] This suggests that juveniles can submit an access request if they are able to understand the content of their data and how they are processed if explained in an age-appropriate way.[929] Young children are not able to access data without their parents or a legal representative acting on their behalf.

As was already mentioned in this study, the decision to collect data from such young children under the Eurodac Regulation was highly controversial in the legislative process, and the practical benefits of doing so were called into question.[930] Guaranteeing data rights is therefore all the more

928 European Commission, 'Can Personal Data about Children be Collected?' (*commission.europa.eu*) <https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en> accessed 24 June 2023.

929 Eurodac Regulation 2024, Art 14 and 42(2); Dix, 'Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services' (n 833), para. 2.

930 E.g., FRA, 'The Impact of the Proposal for a Revised Eurodac Regulation on Fundamental Rights: Opinion of the European Union Agency for Fundamental Rights' (2016); 112 civil society organisations, under the umbrella of European Digital Rights (EDRi) were calling for an end to the expansion of Eurodac in an open letter: 'Civil Society Calls for an End to the Expansion of EU's EURODAC Database' (*edri.org*, 12 April 2023) <https://edri.org/our-work/civil-society-calls-for-an-end-to-the-expansion-of-eus-eurodac-database/> accessed 2 June 2024; according to 6623/23 from General Secretariat of the Council, 'Amended Proposal for a Regulation of the European Parliament and of the Council on the Establishment of "Eurodac" for the Comparison of Biometric Data for the Effective Application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for Identifying an Illegally Staying Third-Country National or Stateless Person and on Requests for the Comparison with Eurodac Data by Member States' Law Enforcement Authorities and Europol for Law Enforcement Purposes and Amending Regulations (EU) 2018/1240 and (EU) 2019/818: 4 Column-Table' (20 February 2023), line 49, the position of the European Parliament of 2022 was, to use data of children to "assist with the protection of child victims of trafficking in human being and the identification and protection of missing children". This narrow use was critisised by some Member States as not allowing for law enforcement access to children's data (8324/23 from General Secretariat of the Council, 'Amended Proposal for a Regulation of the European Parliament and of the Council on the Establishment of "Eurodac" for the Comparison of Biometric Data for the Effective Application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for Identifying an Illegally Staying Third-Country National or Stateless Person and on Requests for the Comparison with Eurodac Data by Member States' Law Enforcement Authorities and Europol for Law Enforcement Purposes and Amending Regulations (EU) 2018/1240 and (EU) 2019/818 - Compilation of Replies by Member States' (20 April 2023), Croatia Line 49).

crucial. All children must be able to access their data, and when a minor submits an access request, the information must be prepared and presented in a way that they can meaningfully absorb it.[931] Member States should ensure that unaccompanied minors receive assistance and legal representation to protect their data protection rights, including their right to access.[932] This is not contained in the Eurodac or Interoperability Regulations. Art. 14 Eurodac Regulation only states that minors have to be accompanied by a representative throughout the time when their biometric data are taken.

Finally, one might ask whether access to Eurodac could be used to help parents whose children have travelled alone to Europe and who have lost contact with them. The collection of fingerprints and facial images from children has been justified with the fact that many migrant children go missing in the Schengen Area.[933] As biographical data are now also stored in Eurodac, parents could request access (e.g., based on a birth certificate) to verify whether their child has arrived in Europe. FRA's survey on biometrics among border guards in six Member States shows that children reported as missing are frequently encountered at border crossing points.[934] Of course, the best interests of the child and their data protection rights

931 GDPR, Recital 58; EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) Version 1.1, section 7; EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 83.

932 CRC, Art 12(1) states that: "States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child." Ibid, Art 12(2) continues that: "For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law." AMMR, Art 11(c) also provides a right to legal counselling and states in Art 13 that "each Member State where an unaccompanied minor is present shall ensure that he or she is represented and assisted by a representative with respect to the relevant procedures provided for in this Regulation." This wording, however, does not explicitly cover the Eurodac Regulation, or does so only insofar as it serves the purposes of the AMMR, which are very limited compared to Eurodac purposes.

933 2016 Eurodac Proposal, 'Explanatory Memorandum,' 4; EU Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), 'Fate of 10,000 Missing Refugee Children Debated in Civil Liberties Committee' *europarl.europa.eu* (21 April 2016) <https://www.europarl.europa.eu/news/en/press-room/20160419IPR23951/fate-of-10-000-missing-refugee-children-debated-in-civil-liberties-committee> accessed 14 June 2024.

934 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 114.

would have to be given priority when considering such access.[935] Moreover, such a function of the Eurodac information system would only be feasible if a procedure with specific conditions for parental access to information on missing children were established. This could take the form of a missing-person report submitted by the parents and forwarded to the responsible police authority. In practice, however, reconnecting through social media, for example, may remain a more likely and practical method for parents to locate missing children. Nonetheless, it may be worthwhile to consider additional functions for Eurodac that serve the interests of the data subjects and their families, and not solely those of the Member States.

cc) Persons with Disabilities

Similar considerations to those above regarding children must be made with regard to persons who, due to impairments, are not able to fully understand data processing procedures within Eurodac and the interoperability system. These may be geriatric people or those with mental disabilities. For them, too, the question arises as to what extent data collection and processing is even permissible, if they are unable to fully understand what happens to the data, especially when processing is not in their best interest. It is rather rare that an adult is legally incapable to exercise a data right, such as access to data (and even if, in most cases, the authorities of a Member State would not necessarily know about this). However, an access to justice approach should take into account the practical hurdles – e.g., a lack of understanding of data processing in highly complex information systems. Persons with disabilities are neither mentioned nor taken into account in the Eurodac and Interoperability Regulations.[936]

935 The controller has to take appropriate measures to avoid any disclosure of personal data of a minor to an unauthorised person (EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 28 para 85); cf also Dix, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 553), para 10.

936 Even though the binding CRPD names accessibility as a general principle in Art 3(f) and as an individual right in Art 9 and holds in Art 12(3): "States Parties shall take appropriate measures to provide access by persons with disabilities to the support they may require in exercising their legal capacity."

dd) Persons outside the Schengen Area

The Eurodac and interoperability systems do not only process data from persons who are located in a Member State. Many data sets concern data subjects who are not (or no longer) in the EU. For instance, if an asylum application is rejected and the individual is returned to a third country, their data will continue to be stored and processed for ten years.[937] The following section examines whether individuals who are no longer present in a Member State have access to their data.

aaa) *Applicability of the Interoperability Regulation*

The Interoperability Regulation applies, according to its Art. 3, to persons in respect of whom personal data may be processed in Eurodac (or any other EU information system or by Europol). It thus applies to data subjects staying outside the Schengen Area, as long as their data are still processed in one of Europe's information systems, like Eurodac. The Interoperability Regulation refers to Art. 15 GDPR with regard to the right to access the MID,[938] adding few additional procedural requirements.[939] Still, the Interoperability Regulation does not provide a special procedure for persons who wish to have access to their data from outside the Schengen Area. This leads to practical problems in implementing access rights, as will be discussed below.

bbb) *Applicability of the Eurodac Regulation*

As stated above, the territorial scope of the Eurodac Regulation is linked to the scope of the AMMR,[940] which applies only in the EU and Dublin-associated countries.[941] The Eurodac Regulation technically contains no legal

937 Eurodac Regulation 2024, Art 29(1).
938 Interoperability Regulation - Judicial Cooperation, Art 48(1) and (11); Interoperability Regulation - Borders, Art 48(1) and (11).
939 ibid, Art 48(1) - (3), (8) and (10).
940 Eurodac Regulation 2024, Art 60.
941 Council Decision of 28 January 2008 on the Conclusion on Behalf of the European Community of the Agreement Between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State

basis on which a data subject outside the Schengen Area could demand access to their data.[942] It hence has to be examined if a person staying outside of the Schengen Area can request access to their data stored in Eurodac.

In general, any data subject has a right to access their personal data stored and/or processed in Europe. Looking at the ECtHR case law, it seems that a right of access to personal data by third-country nationals in cases where data are processed in European databases is provided under Art. 8 ECHR.[943] Furthermore, within the EU the GDPR applies as *lex generalis* with regard to Eurodac data, which is territorially applied whenever data have been processed by a controller or a processor in the EU.[944] Data

---

responsible for examining a request for asylum lodged in a Member State or in Switzerland [2008] OJ L53/3 (Dublin Association Agreement).

942 One could discuss, if the Eurodac Regulation can be applied extraterritorially. However, this is normally only assumed for human rights treaties, cf on this Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press 2011); *Vlastimir and Borka Banković and Others v Belgium and Others* ECHR 2001-XII.

943 Accountability in situations where acts of Contracting States produce effects outside their territory stems from the fact that ECHR, Art 1 cannot be interpreted so as to allow a State Party to perpetrate violations of the Convention on the territory of another State which it would not be permitted to perpetrate on its own territory (European Court of Human Rights, 'Extra-Territorial Jurisdiction of States Parties to the European Convention on Human Rights' (2018) Press Unit 12 and *Ben El Mahi v Denmark* App no 5853/06 (ECtHR, 11 December 2006); cf also Marko Milanovic, 'Foreign Surveillance and Human Rights, Part 3: Models of Extraterritorial Application' (*EJIL: Talk!*, 27 November 2013) <https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-3-models-of-extraterritorial-application/>; Christopher Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (*EJIL: Talk!*, 16 December 2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/>; Evelien Brouwer, 'Extraterritorial Migration Control And Human Rights: Preserving The Responsibility Of The Eu And Its Member States' in Bernard Ryan and Valsamis Mitsilegas (eds), *Extraterritorial Immigration Control - Legal Challenges* (Brill Nijhoff 2010).

944 GDPR, Art 3(1) states that states that the "Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union." The term "main establishment" is defined in ibid, Art 4(16). The GDPR does not provide a definition of "establishment" for the purpose of Art 34. However, ibid, Recital 22 clarifies that an "[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." ibid, Recital 25 states that "[w]here Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as

subjects outside the EU can therefore exercise the right of access to their data on the basis of Art. 3 GDPR or, if their Eurodac data are processed in a Schengen/Dublin-associated country, on the basis of Art. 8 ECHR and, if applicable, national law (some scholars argue that the GDPR may apply in a Schengen/Dublin-associated country under certain circumstances[945]). In the following, we will explore the differences between the right of access under the Eurodac Regulation and that under the GDPR, which may affect the ability of data subjects to exercise this right both inside and outside the EU. The next section will examine general obstacles faced by data subjects located outside the Schengen Area, while keeping in mind that the GDPR remains the applicable law.

ccc) *Access from outside the EU: Is an Ineffective Right Still a Right?*

Identification of Data Subjects

Neither the Interoperability Regulation nor the Eurodac Regulation – which may not apply to data subjects outside the Schengen Area – provides a procedure for how such persons can access their personal data. This absence constitutes an inherent obstacle to the right of access to justice. As seen above, access to data for data subjects outside the Schengen Area is provided through (Art. 48(1) Interoperability Regulation in conjunction with) Art. 15 GDPR, with the Interoperability Regulation providing some additional procedural requirements. There are differences in the scope and mode of access to Eurodac data when a data subject has to exercise the right based on the GDPR instead of the Eurodac Regulation. In any case, data subjects located outside the Schengen Area face multiple barriers that cast doubt on whether they can effectively be recognised as right holders.

First, identifying or authenticating a data subject to grant access to their data is complex when the individual resides outside the Schengen Area. Art. 43(5) Eurodac Regulation stipulates that any request for access to (rectification, completion, erasure or restriction of the processing of personal data) has to contain "all the necessary particulars to identify the

in a Member State's diplomatic mission or consular post." Cf also Daniel Ennöck, 'Artikel 3 - Räumlicher Anwendungsbereich' in Gernot Sydow and Nikolaus Marsch (eds), *Datenschutz-Grundverordnung | Bundesdatenschutzgesetz* (3rd edn, Nomos 2022), para 5; Oskar Gstrein and Andrej Zwitter, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10 Internet Policy Review.

945 See chapter: Schengen-Associated Countries: The Case of Switzerland.

data subject, including biometric". From a data security perspective, asking for biometric identification seems reasonable; this is quite a secure way to identify a person.[946] From an access to justice perspective, however, this can pose an impossible obstacle for a data subject located outside the Schengen Area. Most countries will not be able or willing to provide for the administrative procedure and/or technology to take and transfer fingerprints or facial images to a Member State in a readable format. It is also unclear whether Member States would even accept biometric data if the person does not provide them in person.

According to the GDPR, the controller may "request the provision of additional information necessary to confirm the identity of the data subject", if the controller has reasonable grounds for doubting the identity of the requesting person.[947] This can, but does not have to, include biometric data like fingerprints. The controller must ensure that they do not collect more personal data than is necessary to enable identification of the requesting person.[948] The identification of the requester is important and must be unambiguous in order to avoid the risk of a data breach.[949] Scholars demonstrated that by using publicly available information, e.g., the email address, date of birth, and profile pictures, controllers in some cases can be persuaded to disclose sensitive personal data of the data subject to a malicious third party.[950] The EDPB, too, emphasises that, e.g., copies of ID cards should generally not be considered an appropriate way of authentication.[951] It seems that biometric data would be the safest way to identify the data subject requesting access. The EDPB supports further modes of identification that do not include biometric data, for instance, email or text message that contain confirmation links, security questions, or confir-

946 See for a discussion of the reliability of biometric data, chapter: the Right to an Effective Remedy.

947 GDPR, Art 12(6).

948 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 26 para 70.

949 GDPR, Art 4(12): 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

950 Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR 'Right of Access'', *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (USENIX Association 2019).

951 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 530) 26 para 75.

mation codes.[952] The European Centre for Digital Rights stated that current options for official authentication are very different in the Member States (e.g., some use electronic signatures widely; others have a duty to show a paper ID).[953] Controllers often require one specific way for identification, frequently inspired by the traditions of a certain jurisdiction.[954]

Some of these modes of identification are hardly or not at all accessible to data subjects living outside the Schengen Area, such as showing a paper ID or providing biometric data such as fingerprints. Art. 12(2) GDPR places the burden of proof on the controller to demonstrate that identifying the data subject is impossible.[955] It seems that Member States should offer different modes of identification. And even though, from a data security perspective, asking for fingerprint identification seems reasonable, from an access to justice perspective, this should not be the only option for accessing personal data. Otherwise, data subjects who reside outside the Schengen Area are effectively cut off from the right to access personal data.

If the Eurodac Regulation were applicable to data subjects outside the Schengen Area, they would hardly be able to gain access to data, because of the requirement to provide fingerprints. Under the GDPR, access seems at least theoretically possible. In practice, it is unclear whether access will be provided by Member States. The different practices in the Member States indicate different levels of effectiveness in providing access to personal data.

Legal Address

A second issue is the obligation to provide a legal address. The Eurodac Regulation does not stipulate how information is provided to the data subject. The GDPR also states that a copy of the data has to be provided,[956] which means that the data subject must be given a faithful and intelligible reproduction of all their personal data.[957] That right entails the right to obtain copies of extracts from documents or even entire documents or

952 ibid; cf also Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market [2014] OJ L257/73 (eIDAS Regulation).

953 European Center for Digital Rights, 'Noyb Observations on EDPB Guidelines 01/2022 on Data Subject Rights – Rights of Access (n 556).

954 ibid.

955 Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 467.

956 GDPR, Art 15(3).

957 Case C-487/21 *F.F. v Österreichische Datenschutzbehörde and CRIF GmbH* [2023] para. 54.

extracts from databases,[958] but does not specify whether this has to be in physical or digital form. The EDPB states that the (copy of) personal data and the additional information provided should be in a permanent form such as written text. This should be in a commonly used electronic form, so that the data subject can easily download it.[959] However, downloading information can be a problem if a person does not have access to the internet.[960] For these data subjects, of course, even submitting a request will be very difficult, since they would have to send it physically. Where personal data and information are not provided electronically, they must be sent to the data subject's physical address. In such cases, the data subject is required to provide a (legal) address to receive the information.[961] This can be an obstacle for data subjects who come from regions where the delivery of sensitive documents is hard to provide, such as conflict areas.[962] Moreover, some Member States accept access requests only in paper form and do not provide responses to addresses abroad.[963] This issue affects data subjects outside the Schengen Area, irrespective of the legal basis on which they rely for their access request.

Access to Legal Representation

Finally, for data subjects abroad, understanding the access procedure can be challenging. Furthermore, it will be difficult to find a lawyer who can represent a data subject who is not able to do the request themselves: few lawyers are familiar with these new regulations and procedures, especially outside of the EU.

---

958 ibid.

959 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 15 para 32; according to Bäcker, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 910), para 10, information may be requested in electronic form if the request for information was also submitted electronically.

960 cf International Telecommunication Union, 'Measuring Digital Development - Facts and Figures 2022 International Telecommunication Union Telecommunication Development Sector' (*itu.nit*, 2022) <https://www.itu.int/itu-d/reports/statistics/facts-figures-2022/>, stating that the "[l]atest figures show that an estimated 5.3 billion people of the earth's 8 billion are using the Internet in 2022, or roughly 66 per cent of the world's population".

961 A physical address may also be required to identify the data subject, although it does not necessarily need to be physically accessible for the delivery of documents.

962 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 104.

963 ibid, 104 found that in Poland, replies to access requests that are provided in hard copy within 30 days and they can only be dispatched within the country.

Differences Between the Eurodac Regulation and the GDPR

The applicability of the GDPR to data subjects outside the Schengen Area theoretically allows them to access Eurodac data, even where the Eurodac Regulation itself does not provide for such access. Access may then also not depend on the submission of biometric data, as under Art. 43(6) Eurodac Regulation. However, for access to be genuinely effective, the EU – specifically through the Eurodac and Interoperability Regulations – would need to establish a clear procedure for data subjects outside the Schengen Area. Given the current obstacles, it is highly unlikely that these individuals can practically exercise their right to access their data.

b) *How to Access Personal Data*

aa) Eurodac Data in Eurodac

The Eurodac Regulation contains only a limited number of provisions outlining how the procedure for obtaining personal data should be conducted. The following section examines these provisions, highlighting, as previously, the differences between the Eurodac Regulation and the GDPR in this respect.

aaa) *Requesting Access or Contesting a Decision*

In most cases, a data subject will not make an access request out of sheer curiosity to find out what personal data are stored about them (access might, in such cases, not be granted, as we will see later). Rather, the decision to make an access request normally arises in connection with a decision handed down to the data subject, such as a transfer decision to another Member State. If the data subject claims that this decision is based on incorrect or incomplete data, they might have to first access them. In such cases, confusion can occur between possibilities to appeal the decision and to exercise the right of access.[964] Under the Eurodac Regulation, access is regulated according to Art. 43, which is what this section will analyse. The right to an effective remedy will be discussed in Chapter IV. Data subjects may be required to challenge a decision before a higher court,

964 cf ibid 101.

while simultaneously requesting access to their data through a separate procedure, for instance via the national data protection or asylum authority. This bifurcation of the legal process is not desirable from an access to justice perspective.

Furthermore, some data subjects may not comprehend which data are held in which database. For instance, following a return decision, an alert may be recorded in the SIS, even though the decision relates to an asylum procedure and relies on data stored in Eurodac. Once Eurodac becomes interoperable, distinguishing where specific information is stored will become even more challenging. Certain data collected under the Eurodac Regulation will also be stored in the CIR,[965] templates from biometric data in Eurodac stored in the sBMS[966] and links between data files collected in the MID.[967] This makes it difficult to know how to exercise access rights.

bbb) *Addressee for the Access Request*

The Eurodac Regulation does not determine which Member State is responsible for an access to personal data request. According to the wording of Art. 43(2) Eurodac Regulation, data subjects have an access right in "each" Member State. Art. 43 Eurodac Regulation does not contain a requirement that the Member State answering the request must itself have transmitted or processed data, i.e., be the data controller. A data subject can submit their access request to whichever Member State seems most convenient for them.[968]

According to the GDPR, access can only be requested from the controller, which is whoever "determines the purposes and means of the processing of personal data".[969] Member States designate their controller(s) with regard to Eurodac data. They vary from state to state. It might be the asylum or migration authority, the interior ministry, or a police branch of the Member State that first collected and stored the data subject's personal

965 Eurodac Regulation 2024, Art 3(2); Interoperability Regulation - Judicial Cooperation, Art 17.
966 Interoperability Regulation - Judicial Cooperation, Art 12.
967 ibid, Art 25.
968 Requests for rectification or erasure, which have to be processed by the Member State which transmitted the data are forwarded to the Member State responsible, according to Eurodac Regulation 2024, Art 43(2).
969 GDPR, Art 4(7).

data in Eurodac.[970] There may be multiple controllers involved, for instance if more than one Member State collects data, or if a Member State other than the one that originally collected the personal data becomes responsible for processing it.[971] In practice, data subjects may find it challenging to determine which Member State is responsible for handling their access request. In certain Member States, identifying the competent authority can be particularly difficult, which is likely to cause delays in the access process.[972]

From an access to justice perspective, it is reasonable that under the Eurodac Regulation, the data subject can choose where to submit an access request. In most cases, it will be easiest to submit a request in the Member State where the data subject is staying. However, the regulation also allows the data subjec to submit their request in another Member State, which can be useful if, for example, the data subject speaks the language of that state or has legal representation or other forms of support there. In addition, this allows data subjects to mitigate differences in procedures across Member States. They can submit their access request where it appears to be the simplest and quickest.[973]

---

970 In Germany it is the Bundeskriminalamt (BKA): EU, 'Fingerprints and Eurodac, Information for Third Country Nationals or Stateless Persons Found Illegally Staying in a Member State, Pursuant to Article 29(3) of Regulation (EU) No 603/2013 (EN)' (2014) <https://www.bra.nrw.de/system/files/media/document/file/eurodac-englisch.pdf>;
In Spain the Comisaria General de Policía Cientifíca: EU, 'He Pedido Asilo En La Unión Europea – Qué País Se Encargara de Tartar Mi Solicitud?" Información Sobre El Reglamento de Dublín Para Los Solicitantes de Protección International de Conformidad Con El Artículo 4 Del Reglamento (UE) Nº 604/2013 (Espanol)' (2014) <https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/oficina-de-asilo-y-refugio/Proteccion-internacional/Informacion_Reglamento_Dublin_A_ESPANOL_126140144.pdf>;
In France the Ministère de l'intérieur Direction générale des étrangers en France: EU, 'J'ai Demandé l'asile Dans l'Union Européenne - Quel Pays Sera Responsable de Ma Demande?' Informations Sur Le Règlement de Dublin Pour Les Demandeurs d'une Protection Internationale En Vertu de l'article 4 Du Règlement (UE) N° 604/2013' (2014) <https://www.lacimade.org/wp-content/uploads/2018/01/brochure-dinformation-sur-dublin-III-Fran%C3%A7ais.pdf>.

971 cf EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (Version 2.1, Adopted on 07 July 2021)' (2021).

972 cf FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 51.

973 FRA found, with respect to access requests regarding SIS II, that, "[a]lmost all the competent authorities accept requests in another language than that of the Member State, with only one exception, Poland. In most cases replies are provided in English,

Within a Member State, data subjects are directed to the Eurodac controller to submit their request. Many Member States provide leaflets specifying this administrative authority – often a branch of the police or the Ministry of Interior – and its address.[974] Accessing data through an administrative authority is called 'direct access'.[975] In contrast, some Member States operate a system of 'indirect access,' where the data subject must approach the national data protection authority.[976] A number of countries also provide a dual system, where the national data protection authorities provide for request forms and refer requests to the responsible authority.

ccc) *Identification of the Data Subject*

As previously discussed, Art. 43(6) Eurodac Regulation stipulates that the data subject has to provide biometric data for their identification. This creates particular disadvantages for persons outside the Schengen Area. However, even within the Schengen Area, this requirement can pose a significant hurdle. In many countries, data subjects undergoing procedures,

---

accompanied in some cases by a reply in the national language, but Poland and Italy reply in their national languages only, although Italy is considering introducing the possibility to also answer in English […]" FRA also found that in Poland, replies to access requests that are provided in hard copy within 30 days and they can only be dispatched within the country (FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 104).

974 cf fn 970.

975 cf EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 60 para 198; FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 100.

976 E.g., Commission Nationale de l'informatique et des Libertés, 'Protéger Les Données Personnelles, Accompagner l'innovation, Préserver Les Libertés Individuelles' (2023) Rapport annuel; cf also 'CEDPO - The Confederation of European Data Protection Organisations' <https://cedpo.eu/>; The Italian DPCode also provides for indirect access (through the authority) in case the access could impact with adverse consequence on a number of interests (e.g. interest to contrast money laundering. Cf Italian Personal Data Protection Code [2003] Legislative Decree No 196/2003, Art 2-L; cf for more information on direct and indirect access regarding SIS II and VIS data: SIS II Supervision Coordination Group, 'SIS II Supervision Coordination Group: Activity Report 2013-2015'. Indirect access is sometimes also used to describe an officer or staff member requests another officer or branch to carry out a search. He or she then has to verify if the officer requesting the information is entitled to receive it and, if so, to which information he or she has access and to which not (FRA 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674) 26).

such as asylum procedures, are housed in locations far from major cities. Providing biometric data may therefore require a long journey, which not all data subjects can afford.
Art. 12(6) GDPR is broader and allows for alternative modes of identification. To ensure effective access to personal data, these alternative identification methods should also be made available for requests to access Eurodac data.

ddd) *Form of the Access Request*

Some Member States provide forms or model requests that can be used to submit an access request; in many countries, one can find such letters also provided by NGOs and other organisations.[977] In other Member States, data subjects must formulate their own request. The Eurodac Regulation does not provide details on the form of an access request. In general, access requests do not require any special form.[978]

The Eurodac Regulation allows the right to access data to be restricted under Art. 23 GDPR, particularly when records or a flag suggest the person may pose a threat to internal security.[979] No reasons for rejection are provided for any other type of data. Accordingly, applicants do not seem to be required to justify why they are submitting a request. The EDPB guidelines clarify that data subjects are not required to provide reasons for an access request, and it is not the controller's role to assess whether the request will assist the data subject in verifying the lawfulness of the processing or

977 E.g., Switzerland provides sample letters and a guide on the homepage of the Swiss data protection authority, available at: 'Willkommen beim EDÖB' (*Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter (EDÖB)*) <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/musterbriefe.html>
The French data protection authority also provides for this, available at: Commission Nationale de l'Informatique et des Libertés, 'Besoin d'aide' (n 621);
Germany does not provide a model letter, but instructions on how to do it, at: 'Das Recht auf Auskunft (Art. 15 DSGVO)' (*BfDI*) <https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html> and there are several websites in German, where model letters are provided, e.g. 'Musterbrief Für Anfragen Auf Auskunft Nach Art. 15 DSGVO' (*datenanfragen.de*) <https://www.datenanfragen.de/blog/musterbrief-dsgvo-anfrage-auskunft/>, which also exists in Spanish, English, French, Croatian and Czech.

978 Bäcker, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 910), para 30.

979 Eurodac Regulation 2024, Art 43(3).

exercising other rights.[980] According to the EDPB, assessing the purpose of the request is not appropriate as a precondition for exercising the right of access.[981] The ECJ has affirmed that access must be granted even when the data subject's reasons differ from merely becoming aware of the processing of their personal data or verifying its lawfulness.[982] In contrast, the ECtHR has, in some cases, at least considered the reasons behind an access request.[983] At the national level, courts have, at times, decided that the controller was not obliged to comply with an access request; where it considered it evident that the data subject did not request access in order to be aware of and verify the processing's lawfulness.[984] In practice, it seems

980 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553), 52 para 167.

981 ibid 10 para 13; In the public consultation process regarding the EDPB guidelines it was however pointed out, by Laura Drechsler and others, 'Contribution to the Public Consultation on the Guidelines 01/2022 on Data Subject Rights – the Right of Access' 6, para 2.2, that there is a contradiction between this position of the EDPB and its interpretation of the restrictions of the right to access in GDPR, Art 12(5): "It is hard to see how controllers should on the one hand not consider the 'aim' of data subjects, while on the other, they can use 'malicious' intent to justify not responding to a request [in accordance with ibid, Art 12(5)]"; The CJEU supported the above mentioned understanding of access rights when it decided in Case C-307/22 *FT v DW* [2023] C/2023/1109, that Article 12(5) and Article 15(1) and (3) GDPR "must be interpreted as meaning that the controller is under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of Recital 63 of that regulation."

982 *Addiko Bank d.d. v Agencija za zaštitu osobnih podataka* (n 911); *FT v DW* (n 981).

983 *Dalia v France* [1998] ECHR 1998-I.

984 Rechtbank Rotterdam, 21 january 2020, C/10/576074/HA RK 19-694 (*verzoeker en de Staat der Nederlanden*), no 4.8; Hoge Raad, 16 maart 2018, 17/00173 (*eiseres / verweerder 1 en Stichting Waterlandziekenhuis*), no 3.3.3; Gerechtshof Den Haag, 31 oktober 2017, 200.209.452/01 (*appellant / Bankiers NV)*, no 7; Gerrit-Jan Zwenne, 'Comments - EDPB Guidelines 01/2022 on Data Subject Access, Version 1.0, Adopted on 18 January 2022', states that "[i]t is exactly for this reason that Dutch courts found that the data subject is required to specify such access requests (cf GDPR, Recital 63). In many instances they explicitly ruled that access requests cannot be used for so-called 'fishing expeditions'. The controller is only required to provide access to the extent that the data subjects have sufficiently specified their requests", referring to Gerechtshof 's-Hertogenbosch, 11 december 2014, HV 200.138.190-01 (*appellant 1 en appellant 2 / Coöperatieve Rabobank [regio] UA en Coöperatieve Centrale Raiffeisen-Boerenleenbank BA*), overw. 7.12.5-9, Parket bij de Hoge Raad, 15 januari 2016, 15/01156 (*verzoeker 1 en verzoeker 2 / Coöperatieve Rabobank Weerterland en Cranendonck UA end Coöperatieve Centrale Raiffeisen-Boerenleenbank BA*), no 2.9.1 and Gerechtshof Den Haag, 31 oktober 2017, 200.209.452/01 (*appellant / Bankiers NV*) (n 942), *no 3.7.6.*

that a justification for requesting access may be required in some Member States.

This study aligns with the EDPB's position that, regarding Eurodac data, no justification should be required to grant access. Primarily, this is because, aside from the security flag, the Eurodac Regulation does not specify any grounds for rejecting a request. Consequently, a data subject cannot know which reasons for access would be considered valid or invalid. Secondly, since data subjects registered in Eurodac did not provide their data voluntarily, the threshold for granting access should be kept low.[985]

According to the EDPB, unless explicitly requested otherwise by the data subject, a request to exercise the right of access must be understood in general terms, encompassing all personal data concerning the data subject.[986] Some scholars claim that an access request must enable the controller to find the information they are supposed to disclose. In the case of extensive data processing, the controller should be able to require the data subject to specify the information or processing operations to which his or her request for information relates.[987] With regard to Eurodac, this could pose a problem: some data subjects may not know for what purposes their data are used within the interoperable Eurodac, especially with regard to functions that are provided in the Interoperability Regulation. The extent to which controllers must provide information on the purposes of data processing when responding to an access request will be discussed in the next section. From an access to justice perspective, a data subject submitting a general access request should receive enough information about what is stored and processed in Eurodac. This would allow them to make an informed

985 Eurodac Regulation 2024, Art 12(2) entails a specific obligation for the controller to facilitate the right to access personal data; cf also Alexander Dix, 'Article 12 - Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection regulation: Article-by-Article Commentary* (Nomos 2023), para 16.

986 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 16 para 35; Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 464.

987 GDPR, Recital 63; Bäcker, 'Artikel 15 - Auskunftsrecht der betroffenen Person' (n 910), para 30; Alexander Dix, 'Article 15 - Right of Access by the Data Subject' (n 662) para 5.

decision about which specific data they might want to request in a second step.[988]

Making a request for access to personal data can be a challenge for data subjects, especially when the responsible authority does not provide model letters. In a study by FRA, public authorities and providers of legal assistance from different EU countries have concurred that it may often be necessary for data subjects to hire a lawyer to comply with the procedures for exercising the right of access, deletion, and correction.[989] Providers of legal assistance also report difficulties in understanding the rules governing EU information systems, highlighting a lack of expertise and knowledge in this area.[990]

eee) *Fee for the Access Request*

The Eurodac Regulation does not state whether a fee can be charged for access to personal data. Differently, Art. 12(5) GDPR stipulates that access is generally provided free of charge. Controllers can charge only "a reasonable fee" for requests that are manifestly unfounded or excessive, in particular because of their repetitive character,[991] or where further copies are requested.[992] Since the access right in the Eurodac Regulation has to be exercised in accordance with Chapter III of the GDPR, the provisions regarding fees are applicable.[993] Furthermore, the ECJ decided that "in order to ensure

988 According to Dix, 'Article 15 - Right of Access by the Data Subject' (n 662) para 5, if the request of specifying the information or processing activities is not complied with, the controller will have to give complete access.

989 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 102.

990 ibid 102; This also seems to be reflected in the fact there have been very few accesses to information requests with regard to Eurodac over the past years. The transaction type for access to Eurodac data is called a Category 9 search. In 2020, 102 Category 9 searches were performed. Since 2017, the number of access applications has fluctuated between just under 100 and a good 200 per year (eu-LISA, 'Eurodac 2021 Annual Report' (2022) 25). In 2021 the number rose to 224 category 9 searches and in 2022 to 342, i.e. access requests (ibid 25).

991 GDPR, Art 12(5).

992 ibid, Art 15(3).

993 The provision can be considered *lex generalis*; according to the Eurodac SCG, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (n 694) 8, Q 10: "As regards possible fees, the majority of Member States do not charge any fee for paper copies. Additionally, two Member States apply an administrative fee for the copy of the file."

that fees levied when the right to access personal data is exercised are not excessive […], the level of those fees must not exceed the cost of communicating such data".[994] The ECJ has ruled that when personal data are being processed, the controller must provide the data subject with a first copy free of charge. This obligation applies even if the request is not intended to verify the lawfulness of the processing or to become aware of it.[995]

fff) *Restriction of the Right to Access*

There is, as mentioned, only one restriction to the right of access encompassed in the Eurodac Regulation with regard to security flags.[996] This is different from the right to access in Art. 15 GDPR, which can be restricted, based on either Art. 15(4), Art. 12(5) or Art. 23 by way of legislative measures in Union or Member States law. Several Member States have made use of the latter option.[997]

If, as this study argues, the right of access is interpreted broadly – meaning that data subjects should, in principle, be informed about law enforcement access or transfers to third countries – certain restrictions must nonetheless apply. For example, it must be ensured that ongoing criminal procedures or investigations are not jeopardised.[998] De facto, this restriction already exists even though it is not explicitly mentioned in the Eurodac Regulation, as long as access to information – such as whether national law enforcement authorities or Europol have accessed the personal data – is not guaranteed.

---

994 Case C-486/12 *Judgment of the Court (Eighth Chamber) in the proceedings brought by X* [2013] OJ C 45/13, para 31.

995 *FT v DW* (n 981), para 23 and 80.

996 Eurodac Regulation 2024, Art 43(3). As mentioned above, according to the ECJ in *Ligue des droits humains* (n 876), para. 70, national (supervisory) authorities must document why a restriction has been invoked, even in cases involving national security; however, the German National Implementation Plan 'Nationaler Implementierungsplan (NIP) für Deutschland' 9 (n 615) states that information provided to data subjects does not extend to matters relevant to security.

997 cf for example Sections 32 to 37 of the German Federal Data Protection Act (Federal Data Protection Act, as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045) [2017] (BDSG)), where restrictions are allowed if information would endanger the proper performance of tasks or endanger public security or order. Cf also the Personal Data Protection Act (Poland) [2018], Art 5 and 5a; for more information cf EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 51, para 165ff.

998 cf GDPR, Art 23(1)(d), (f).

ggg) *Time Limit for an Answer to the Request*

The Eurodac Regulation does not provide a time limit within which an access request must be answered. This is different from the GDPR, which sets a one-month deadline, extendable by up to two additional months.[999] It is unclear whether the *lex specialis*, the Eurodac Regulation, deliberately deviates from the *lex generalis,* the GDPR, by not setting a time limit. In practice, no such deliberate divergence appears to exist. The SCG Eurodac reported that, with regard to time limits for responding to an access request, most Member States have established a maximum of 30 days. In some Member States, the time limit is even shorter, such as 8 or 15 days.[1000] Several Member States reported that the limit may be extended when necessary, taking into account the complexity and the total number of requests.[1001] This contrasts with a FRA study, which indicates that, for access requests concerning SIS II and VIS data, authorities often take significantly longer than one month to respond.[1002] The Eurodac Regulation also does not specify that requests must be answered within a "reasonable time," a standard that data subjects could otherwise invoke.[1003]

hhh) *Form of the Data Provided*

The Eurodac Regulation does not specify the form in which data must be provided. According to Art. 43(2) Eurodac Regulation, data subjects can "obtain communication of the data relating to him or her recorded in Eurodac including any record indicating that the person could pose a threat to

999 ibid, Art 12(3).

1000 Eurodac SCG, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac' (n 694) 8, Q 10.

1001 ibid 8, Q 10.

1002 cf FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 103.

1003 CFR, Art 41(1) provides this for affairs to be handled within reasonable time by the institutions, bodies, offices and agencies of the Union (The general principles of EU law bind the EU institutions, bodies, offices and agencies, and also, Member State institutions when they act within the scope of EU law (Craig, 'Article 41 - Right to Good Administration' (n 880), para 41.02); The reasonable time-requirement also forms part of the right to a fair trial according to Art. 6 ECHR, which, however, only applies to judicial proceedings (ECtHR, 'Guide on Article 6 of the European Convention on Human Rights: Right to a Fair Trial' (2017) 66ff, para 352ff).

internal security, and the Member State which transmitted them to Eurodac […]." There is no definition of 'communication' in the Eurodac Regulation. The GDPR, on the other hand, allows for "access to the personal data". It stipulates that a copy of the data has to be provided.[1004] A copy means that the data subject must be given a faithful and intelligible reproduction of all their personal data.[1005] That right entails the right to obtain copies of extracts from documents or even entire documents or extracts from databases.[1006] The obligation to provide a copy strengthens the right of access.[1007] Furthermore, there is no right to data portability in the Eurodac Regulation. Data portability, according to Art. 20 GDPR, means that the data subject has a right to receive data in a structured, commonly used, and machine-readable format. The data subject has the right to transmit those data to another controller.

The drafting history of the Eurodac Regulation does not clarify why the term 'communication' was introduced. The provision has been rephrased in the latest revision to clarify the rights of data subjects, due to concerns of its unclarity in earlier versions, which were raised by the EDPS already in 2009 and 2011.[1008] The wording, with regard to the access right, was not changed from earlier versions.[1009] Even though 'communication' and not a copy of the data can be obtained, it is argued here that the personal data still have to be "easily visible, intelligible and clearly legible".[1010] In a

1004 GDPR, Art 15(1) and (3).
1005 *F.F. v Österreichische Datenschutzbehörde and CRIF GmbH* (n 957) para. 54.
1006 ibid.
1007 Zanfir-Fortuna, 'Article 15 - Right of Access by the Data Subject' (n 858) 464.
1008 cf EDPS, 'Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of Regulation (EC) No […/…] (Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person) (COM(2008)825)' (2009) OJ C 229/6, paras 36 - 38; EDPS, 'Opinion of the European Data Protection Supervisor on the Amended Proposal for a Regulation of the European Parliament and of the Council on the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of Regulation (EC) No (…/…) (Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person)(2011/C 101/03)' (2010) OJ C 101/14, paras 26 - 29.
1009 cf Eurodac Regulation 2000, Art 18(2); Eurodac Regulation 603/2013, Art 29(4).
1010 GDPR, Art 12(7).

ruling by the ECJ, the German Court asking for preliminary ruling argued in connection with access to a digitised asylum file that the representative of the person concerned must have the same display of information as the court.[1011] The ECJ stated that the "method of communication" has to guarantee "a faithful reproduction, as far as possible, of the structure of that file and the chronology of the submission of the various documents".[1012] This requirement reflects the principle of equality of arms and should likewise apply to Eurodac files. Personal data or 'communication', it is argued here, must be displayed in the same way as they are displayed to the authority that processes it. They must be readable and understandable to the data subject.

bb) Eurodac Data in the Interoperability System

The Interoperability Regulation establishes its own system for access, rectification, erasure, and restriction of processing requests. Under the Interoperability Regulation, access requests must be submitted in a web portal, according to Art. 49 Interoperability Regulation. Recital 69 of the Interoperability Regulation states, that "[a]s the interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data are processed through those components can effectively exercise their rights […]." Therefore, a web portal will facilitate the exercise of the rights of access to, rectification, erasure, and restriction of personal data.[1013] The web portal will be established and managed by eu-LISA.[1014]

According to Art. 49(2) Interoperability Regulation, the web portal only enables persons who have been informed of the presence of a red link to

1011 Case C-564/21 *BU v Federal Republic of Germany* [2022] OJ C 35/14, para 48: "According to it, that method of communication does not comply with the right to a fair trial enshrined in the second paragraph of Article 47 of the Charter. In particular, it points out that, since the display of all the documents in PDF format transmitted by the administration in chronological order requires the downloading of specific software, it cannot be ruled out that that display is different for the competent court and for the representative of the person concerned, so that the availability of a file of identical content and form to all the parties to the asylum procedure concerned is not guaranteed."

1012 ibid, para 50.

1013 Interoperability Regulation - Judicial Cooperation, Art 49(1).

1014 ibid, Art 49(5).

make a request through this tool. Where the MID created a red link, the data subjects concerned are informed about this[1015] and will need to verify their identity via the web portal.[1016] Data subjects enter the reference of their identity confirmation file, indicating in which EU information system the linked data are held.[1017] The web portal uses this reference in order to retrieve the contact information of the competent authority of the Member State responsible for the manual verification of different identities. The web portal will also include a template e-mail to facilitate communication between the portal user and the competent authority.[1018]

In cases where no red link was created, data subjects have to, it seems, find out for themselves which authority is responsible for their request and address them.[1019] They will not be able to use the web portal for this purpose. A data subject may submit their access request in any Member State. While any Member State appears competent to grant access to personal data, only the Member State responsible (for the data) can rectify or erase it

1015 In accordance with ibid, Art 32(4): "Without prejudice to the provisions related to the handling of alerts in SIS contained in Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, where a red link is created, the authority responsible for the manual verification of different identities shall inform the person concerned of the presence of multiple unlawful identity data and shall provide the person with the single identification number referred to in Article 34(c) of this Regulation, a reference to the authority responsible for the manual verification of different identities referred to in Article 34(d) of this Regulation and the website address of the web portal established in accordance with Article 49 of this Regulation".

1016 ibid, Art 49(2).

1017 ibid, Art 49(3) in conjunction with ibid, Art 34(b).

1018 Interoperability Regulation - Judicial Cooperation, Art 49(3).

1019 ibid, Art 49(2) *e contrario* in conjunction with ibid, Art 48(1). However, the EDPS, in: EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), para 121 and 123, points out that "in this respect, the EDPS observes that when an individual would submit a request to any Member State as it is laid down in Art. 47(1) of the Proposals, this Member State would have to assess who is the responsible Member State for the manual verification. However, since in Art. 13(2) [the sBMS] and Art. 18(2) [the CIR] of the Proposals merely refer to the relevant system but not the Member State responsible, the Interoperability Regulation - Judicial Cooperation, Art 26(2) limits the access of the Member State to Identification confirmation file in this respect."; cf also FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 51.

following such a request.[1020] If a request for rectification or erasure is made to a Member State other than the Member State responsible for the manual verification, or in cases where the ETIAS Central Unit was responsible, the Member State to which the request has been made contacts the responsible authority.[1021]

As was explained above, the Interoperability Regulation only provides a legal basis for access, rectification, erasure, or restriction of processing requests to the MID, but not the CIR or sBMS. One could consider trying to base a request for access to (or rectification, erasure, or restriction of processing in) the CIR or sBMS on the *lex generalis* in Art. 15, 16 or 17 GDPR respectively or directly on Art. 8 CFR or Art. 8 ECtHR.[1022] Whether access would indeed be granted, is unclear. In any case, a fragmentation of legal protection is undesirable from an access to justice perspective. In practice, this will very likely lead to less effective access.

The Interoperability Regulation sets a 45-day period for responding to rectification or erasure requests.[1023] However, the provision makes no reference to requests for access and restriction. As explained above, the Interoperability Regulation refers to the GDPR with regard to the right to access personal data. It could therefore be argued that the shorter, 30-day deadline established under Art. 12(3) GDPR applies.

1020 Interoperability Regulation - Judicial Cooperation, Art 48(3); EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), para 120: "The EDPS observes that Article 47(1) of the Proposals provides with regard to the data subjects' right of access, the rights to rectification, erasure and restriction that the data subject can send his or her request to any Member State, which shall examine and then reply to the relevant request."; Art. 29 WP 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 15, states that: "[…] any person should be able to address him or herself to any Member State, the Member State to which the request has been made".

1021 Interoperability Regulation - Judicial Cooperation, Art 48(3) and (4). There is no obligation contained in this article for the Member State to inform the data subject that his or her request was forwarded, while indicating the contact details of the competent authority in the relevant Member State. This would allow the data subject to identify the competent authority more easily and would enable the data subject to address further requests directly to the responsible authority. The lack of such an obligation has therefore been critizised by the EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), no 124.

1022 cf section D.II.1.: What Is the Right to Access Personal Data?

1023 Interoperability Regulation - Judicial Cooperation, Art 48(2).

Data subjects must be informed in writing about the rectification or erasure of data.[1024] If a Member State is not prepared to rectify or erase data, it must adopt a written administrative decision.[1025] The fact that requests for access are not explicitly mentioned here could be interpreted to mean that, in principle, they may not be rejected. As explained above, this study maintains that no reasons need to be provided for submitting requests for access. Consequently, such requests cannot be rejected on that basis. What remains possible, however, is to withhold part of the data that the data subject requested. In such instances, decisions must include information explaining the possibility to challenge this, in accordance with Art. 48(8) Interoperability Regulation.

Access requests must include the information necessary to identify the data subject. The Interoperability Regulation does not specify which information must be used for identification; for this reason the *lex generalis*, Art. 12 GDPR, can be consulted. As described above, the GDPR does not require a specific type of identification, such as biometric data. Similar to the Eurodac and Interoperability Regulations, it does not establish a procedure for accessing personal data when the data subject resides outside the EU. Many of the difficulties mentioned earlier therefore still apply, even if the data subject is not always required to identify themselves using biometric data. The web portal addresses some of these issues, but its limited use means that many access requests by persons outside the Schengen Area will likely continue to face obstacles in exercising their rights.

cc) Conclusions

Data subjects might have to make parallel requests based on the Eurodac Regulation, the Interoperability Regulation and the GDPR, depending on what information they want to access and where they are located. They will have to travel and provide biometric data, if they want to access data in Eurodac. Depending on where the data subject submits the request, procedures can vary. Some Member States provide user-friendly model forms, while others require self-written requests. They may ask for reasons for the request and specify the exact information the data subject seeks. A

1024 ibid, Art 48(5). Member States also have to keep a written record of each request and of how it was addressed. They must make that record available to supervisory authorities without delay (ibid, Art 48(10)).

1025 Interoperability Regulation - Judicial Cooperation, Art 48(7).

response to a Eurodac data access request can legally be expected within a defined time period, although in practice this is not always adhered to.

One way to make access procedures in the Schengen Area more accessible and harmonised would be for all national data protection authorities to provide model forms for access requests and to have the authority to receive such requests and forward them to the competent authority. Another idea, brought forward by FRA, suggests an EU-wide request handling mechanism to manage access, rectification, and erasure of personal data requests as well as to provide information on how to initiate and follow up on them.[1026] This, according to FRA, could have been achieved through the establishment of an EU web-portal managed by eu-LISA.[1027] Others suggest a complaints mechanism, based on the EBCG model[1028] and with the involvement of the EDPS; enabling individuals affected to seek administrative review.[1029] So far, nothing of the sort exists.

c) *What Information Can Be Accessed?*

aa) Under the Eurodac Regulation

The Eurodac Regulation does not provide a list of data that have to be accessible to the data subject under Art. 43. It provides such a list only with regard to the right to information in Art. 42.[1030] This chapter argues that the

1026 FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 51.

1027 ibid 51.

1028 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard [2016] OJ L251/1 (EBCG Regulation 2016).

1029 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 414ff.

1030 Eurodac Regulation 2024, Art 42 refers to the identity and contact details of the controller; data to be processed in Eurodac and the legal basis for processing, including a description of the aims of the AMMR and where applicable the Resettlement Regulation and an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes; the fact that a person could pose a threat to internal security; recipients or categories of recipients of the data; the obligation to have biometric data taken; the storage period; the existence of the right to access, rectification and erasure and right to lodge a complaint with the supervisor authority. This list omits the purposes for which data is being processed, the sources of data not collected from the data subject and the existence of automated decision-making including

list of information in Art. 42 Eurodac Regulation contains some of the data but not all that should be accessible under Art. 43 Eurodac Regulation.

aaa) *Personal Data Relating to Him or Her*

The Eurodac Regulation, as said, does not provide a list of data that have to be accessible to the data subject under Art. 43. According to Art. 43(2) Eurodac Regulation, data subjects can obtain communication of the "personal data relating to him or her recorded in Eurodac, including any record indicating that the person could pose a threat to internal security, and of the Member State which transmitted them to Eurodac […]." This is different from Art. 15 GDPR which provides a list of data that can be accessed.

The Eurodac Regulation narrows down the information that can be accessed to personal data "recorded in Eurodac". No difference is made between data that are recorded in the CIR and data recorded in the Central System of Eurodac.[1031] The data subjects must thus have access to all the data listed in Art. 17 Eurodac Regulation. This includes all the biographic and biometric data, as well as information like the conditions for entering a security flag, information on whether an identity document is considered to be authentic, dates of arrivals, transfers or the taking of biometric data, whether the application for international protection has been rejected, etc.

The Eurodac Regulation refers to "personal data relating to him or her". 'Personal data' in the sense of the GDPR means "any information relating to an identified or identifiable natural person ('data subject') […]."[1032] The concept of 'personal data' must be understood as wide in scope. It is not restricted to information that is sensitive or private. Potentially, it encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.[1033] This condition is satisfied where the information, by reason of

meaningful information about the logic involved, which are included in the GDPR list.

1031 ibid, Art 3(2) provides which of the data collected according to ibid, Art 17 is stored in the CIR, providing that the remaining Eurodac data shall be stored in the Central System.

1032 GDPR, Art 4(1).

1033 Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] OJ C 72/20, para 34; but also: *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), para 40ff; Art. 29 WP, 'Opinion 4/2007 on The Concept of Personal Data' (n 560); Lynskey, 'Decon-

its content, purpose or effect, is linked to a particular person.[1034] The ECJ also states that data subjects have a right to obtain a complete copy of the documents containing personal data if the copy is necessary to enable the data subject to verify the accuracy and completeness of the data.[1035]

One of the main discussions around personal data is the distinction from non-personal data. The dualism between these two categories has been increasingly challenged.[1036] In its recent case law, a trend towards a relative approach by the CJEU has been visible.[1037] According to this relative approach, data are not 'personal' or 'non-personal' by nature. Their legal qualification depends on the ability of the organisations who hold them to re-identify them. In one case, for example, the Court decided: even if data could be considered as pseudonymised (and thus personal data according to the EDPS),[1038] one should consider whether the recipient of that data could (reasonably and lawfully) get the additional information needed to

---

structing Data Protection in the EU Legal Order: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (n 553); EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 35, para 106; Two distinctions regarding the range of data falling within the scope of both rights can be observed: first, unlike the notion of 'privacy interference', the concept of 'personal data' is not context dependent and, second, the concept of personal data includes data relating to unidentified yet identifiable individuals.

1034 *Peter Nowak v Data Protection Commissioner* (n 1033), para 35.

1035 *Addiko Bank d.d. v Agencija za zaštitu osobnih podataka* (n 911), para 2.

1036 Bárbara da Rosa Lazarotto and Gianclaudio Malgieri, 'The Data Act: A (Slippery) Third Way beyond Personal/Non-Personal Data Dualism?' (*European Law Blog*, 4 May 2023) <https://europeanlawblog.eu/2023/05/04/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/> accessed 5 May 2023, claims that "the difference between 'personal data' and 'non-personal data' is more and more challenged and in some EU Acts this dualism is softened. Two clear examples are the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance [2022] OJ L152/1 (Data Governance Act)) from 2022 and the Proposed Data Act (Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data [2022] COM(2022)68 (Proposed Data Act))".

1037 Alexandre Lodie, 'Case C-479/22 P, Case C-604/22 and the Limitation of the Relative Approach of the Definition of "Personal Data" by the ECJ' (*European Law Blog*, 25 March 2024) <https://europeanlawblog.eu/2024/03/25/case-c-479-22-p-case-c-604-22-and-the-limitation-of-the-relative-approach-of-the-definition-of-personal-data-by-the-ecj/>.

1038 Case T-557/20 *SRB v European Data Protection Supervisor* [2022] Oral intervention of the European Data Protection Supervisor; or EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 21 para 45.

re-identify them in order to qualify data as personal.[1039] This approach has been outlined in the ECJ's Breyer case.[1040] In another case, P *OC v European Commission,* the ECJ explicitly stated that the fact that additional information originates from a person or source other than the controller of the data in question does not, in any way, negate the identifiable nature of a person.[1041] In yet other recent case law, the Court followed a more objective approach, considering pieces of data as 'personal' without testing whether they are re-identifiable.[1042]

With regard to Eurodac data, this means that, for example, the information that a data subject's family member has applied for asylum in a certain Member State may also count as "data relating to him or her". Data relating to someone may also mean information, comments, or an analysis[1043] related to the personal data collected by a Member State, e.g., with regard to whether a person is "violent", as required for a security flag.[1044]

1039 *SRB v European Data Protection Supervisor* (n 1038), paras 99, 102 and 104ff; for more on this case: Alexandre Lodie, 'Are Personal Data Always Personal? Case T-557/20 SRB v. EDPS or When the Qualification of Data Depends on Who Holds Them' (*European Law Blog*, 7 November 2023) <https://europeanlawblog.eu/2023/11/07/are-personal-data-always-personal-case-t-557-20-srb-v-edps-or-when-the-qualification-of-data-depends-on-who-holds-them/> and Case C-479/22 P *OC v European Commission* [2024], para 53.

1040 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C 475/3.

1041 P *OC v European Commission* (n 1039), para 55. In this case the Court had to consider whether a press release was to be considered personal data, it recalled that, for data to be considered personal data, it is not necessary that people be identified directly from the information contained in the press release. The Court adds in para 56: "Regulation 2018/1725 does not lay down any conditions as regards the persons capable of identifying the person to whom an item of information is linked, since Recital 16 of that regulation refers not only to the controller but also to 'another person'".

1042 Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] C/2024/2907.

1043 cf Dix, 'Article 15 - Right of Access by the Data Subject' (n 662), para 14; EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 35 para 106: "The words "personal data concerning him or her" should not be interpreted in an "overly restrictive" way […]".

1044 Eurodac Regulation 2024, Art 17(2)(i); 22(3)(d), 23(3)(e) and 24(3)(f).

aaa) *Eurodac Hit*

A Eurodac hit, indicating that personal data of a person are already stored in Eurodac, constitutes personal data in the sense of Art. 4(1) GDPR.[1045] It is thus argued here that data subjects should be able to access information as to how the hit was produced, i.e., what biometric (or other) data were compared and, in some cases, information on the mode of comparison or an expert verification, respectively.

According to Art. 27 Eurodac Regulation, comparison within Eurodac is made with biometric data by any Member State, not specifying which biometric data. Art. 38(1) Eurodac Regulation adds that Member States shall ensure the transmission of biometric data of an appropriate quality for the purposes of comparison by means of the computerised fingerprint and facial recognition system. If available, both fingerprints and facial images, it seems, are compared in the Eurodac system. Art. 28(1) Eurodac Regulation states that facial image comparison is made whenever the quality of the fingertips does not allow for appropriate comparison or when no fingerprints are available.

Under the new Eurodac Regulation – and different from Eurodac Regulation 603/2013[1046] – the results of fingerprint comparison are not always checked by a fingerprint expert, but only "where necessary".[1047] Once a hit is produced for both fingerprints and facial images, Member States may check the result of the comparison of the facial image data. Only if a Eurodac hit is based solely on comparison of facial images, shall "an expert trained in accordance with national practice" immediately check and verify the result of the comparison.[1048]

1045 Art. 29 WP, 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 13: "The so-called "hit-flag" indicating that data on a person are stored in the CIR, constitutes personal data." A hit indicating that data is stored in Eurodac must, accordingly, also be considered personal data.

1046 Eurodac Regulation 603/2013, Art 25(4).

1047 Eurodac Regulation 2024, Art 38(4).

1048 ibid, Art 38(5); According to the 2016 Eurodac Proposal, Art 42(4), a feasibility study should have been done by 2020 to evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of Eurodac. The framework of the study, which will only evaluate the reliability and accuracy of the results produced from facial recognition software for the purpose of Eurodac, was furthermore critisised by the EDPP for lacking an analysis of the necessity and proportionality of the processing of facial images (D1736 from Wiewiórowski

Whenever an expert has verified a Eurodac hit, such verification should be available to the data subject; this is considered personal data and might be essential to be able to challenge the result of a hit. If it was not deemed "necessary" to have the hit checked by an expert, the data subject must still receive comprehensible information as to how the hit was generated. According to the ECJ, personal data should be presented to the data subject in the same format as it is shown to the authority processing it, and it must be readable and understandable to the data subject.[1049] It is not enough, it can be argued, to just tell a data subject that the hit was produced by a reliable, computerised fingerprint and facial recognition system.

For law enforcement purposes, designated authorities and Europol may submit a request for the comparison of biometric *or* alphanumerical biographic data.[1050] With alphanumeric data, it is generally much easier to verify the results of a comparison. Nevertheless, there will be hits that do not yield a 100% match. For example, a name may be spelled differently, a place of birth may vary, or dates of birth may be similar but not identical. The more data points are used in the comparison, the more reliable the outcome becomes. With less data, the result must be assessed; a judgment must be made as to whether the person can be identified. In this case, the data sets compared and the result of any assessment should be provided to the data subject.

- EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298)). So far, the study has not been conducted.

1049 *BU v Federal Republic of Germany* (n 1011), para 48: "According to it, that method of communication does not comply with the right to a fair trial enshrined in the second paragraph of Article 47 of the Charter. In particular, it points out that, since the display of all the documents in PDF format transmitted by the administration in chronological order requires the downloading of specific software, it cannot be ruled out that that display is different for the competent court and for the representative of the person concerned, so that the availability of a file of identical content and form to all the parties to the asylum procedure concerned is not guaranteed".

1050 Eurodac Regulation 2024, Art 33(1) and 34(1).

bbb) *Security Flag*

Following the health, vulnerability, identity, and security checks as held in the Screening Regulation,[1051] the AMMR,[1052] and the Asylum Procedure Regulation,[1053] the fact that a person could pose a threat to internal security (according to Art. 15 Screening Regulation) is recorded in Eurodac if the person is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in the Terrorism Directive or in any of the offences referred to in the EAW Council Framework Decision."[1054] Persons considered a security threat may be excluded from relocation in conformity with the rules in the AMMR.[1055] Furthermore, for flagged applicants, assessors are required to focus first on whether this flag may amount to an exclusion or rejection ground.[1056] According to Art. 42(1)(c) Eurodac Regulation, the data subject concerned has to be informed about the fact that they are considered to be a potential threat to internal security. They must also be told that the Member State of origin is obliged to register that fact in Eurodac. The question hence is: which information exactly does the data subject have access to?

As discussed in the previous chapter, the Eurodac Regulation does not clarify what specific information will be stored in Eurodac regarding the security flag. Art. 15(1) Screening Regulation states that a security check may include both third-country nationals and the objects in their possession. A security flag is generated when a hit is obtained from comparing personal data, including biometric data, from the data subject[1057] with any EU migration information system, including the ETIAS watch list.[1058] Compairson is also made with personal data processed by Europol, which

1051 Screening Regulation, Art 12 and 14-16.
1052 AMMR, Art 8(4).
1053 Eurodac Regulation 2024, Art 17(2)(i), 22(3)(d), 23(3)(e) and 24(3)(f) in conjunction with the Screening Regulation, AMMR and the Asylum Procedure Regulation.
1054 Eurodac Regulation 2024, Art 17(2)(i) and Recital 8. The list of offences covered by this directive is much shorter than was the case with earlier drafts of the new Eurodac Regulation. However, this limitation is offset by the potentially very broad and defined only in ibid, Recital 8, as "whether the person has displayed behaviour that results in physical harm to other persons that would amount to a criminal offence under national law".
1055 AMMR, Art 57(2).
1056 D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 2.
1057 Screening Regulation, Art 9.
1058 ETIAS Regulation, Art 34.

is used to identify connections or other relevant links between information[1059] and Interpol databases.[1060] Also, relevant national databases may be consulted.[1061] Data subjects who shall be relocated receive a form that indicates that a hit has been produced, labelling them a security threat.[1062] It is unclear whether the form shows which database produced such a hit. Data subjects who are not relocated seem not to receive the form.[1063]

The Eurodac Regulation introduces three additional criteria, as mentioned above. At least one of these criteria must be met for a data subject to be registered as a potential threat in Eurodac.[1064] Other than the security flag itself, the fact that a person is violent or unlawfully armed, or where there are clear indications that the person is involved in a criminal offence will have to be recorded. As detailed in the next chapter, such entries must be supported by some form of evidence. For instance, Recital 8 of the Eurodac Regulation specifies that, in assessing whether a person is unlawfully armed, a Member State must determine if the individual is carrying a firearm without a valid permit or authorisation, or any other type of prohibited weapon as defined by national law. The result of such an assessment should be recorded in Eurodac.

So, what information should be accessible to data subjects? To answer this question, it might be enlightening to consider what type of information security flags are. Galli has pointed out that security flags could be considered police information or intelligence information.[1065] The lack of

1059 Europol Regulation, Art 18(2).

1060 Screening Regulation, Art 15(2) in conjunction with ibid, Art 16(6) and Interoperability Regulation - Borders, Art 9(5) and 72(1).

1061 Screening Regulation, Art 15(2). ibid, Art 12(3) provides that "as regards the consultation of EES, ETIAS with the exception of the ETIAS watchlist, and VIS pursuant to paragraph 2, the retrieved data shall be limited to indicating refusals, annulment or revocation of a travel authorisation, refusals of entry, or decisions to refuse, annul or revoke a visa or residence permit respectively, which are based on security grounds. In case of a hit in the SIS, the screening authority carrying out the search shall have access to the data contained in the alert". Ibid, Art 15(4) adds that "as regards the consultation of the ECRIS-TCN system, the data retrieved shall be limited to convictions related to terrorist offences and other forms of serious criminal offences referred to in Article 5(1)(c) of Regulation (EU) 2019/816."

1062 Screening Regulation, Art 17(1)(h).

1063 ibid, Art 18(3) *e contrario* and ibid, Art 18(2), (4).

1064 Eurodac Regulation 2024, Art 17(2)(i).

1065 Galli, 'Interoperable Databases: New Cooperation Dynamics in the EU AFSJ?' (n 73) 124.

classification leads, according to Galli, to problems. If the flagging is classified as police information, the process for adding a flag must be disclosed. This includes details on how the assessment was made and the information used.[1066] Such a disclosure should occur as soon as the data subjects are informed about the flag. Ideally, it should happen even earlier. In the case of intelligence information, disclosure would have to occur much later, once any potential danger posed by the data subject has passed.[1067] This is compounded by the fact that national security falls outside EU competence under Art. 4(2) TFEU. While interstate cooperation within the AFSJ is formally limited to police matters, intelligence sharing – related to national security – does not fall within EU competence.[1068]

The three criteria set out in the Eurodac Regulation appear to constitute police information; whether someone is violent, unlawfully armed or where there are clear indications that the person is involved in an offences are police information. Each of these facts should prompt a police investigation and may, where appropriate, result in an indictment by the public prosecutor. In contrast, if someone is registered, in a Europol, Interopol or national security intelligence database, this is intelligence information.

The Eurodac Regulation provides that access can be restricted in accordance with Art. 23 GDPR.[1069] Controllers may invoke a restriction to the extent that it is explicitly provided for in Union or Member State law.[1070] Without the corresponding legislative measure, controllers cannot rely directly on the grounds listed in Art. 23(1) GDPR.[1071] The domestic law

1066 ibid 124.
1067 ibid 124.
1068 ibid 121.
1069 Eurodac Regulation 2024, Art 43(3). Security related restriction also occur in other information systems, like Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the Establishment, Operation and use of the Schengen Information System (SIS) in the Field of Border Checks [2018] OJ L312/14 (SIS III - Borders Regulation), Art 52(2) and Amendment to the VIS Regulation 2021, Art 38(7).
1070 EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (2021) Version 2.1, 7 para 16; Dominique Moore, 'Article 23 Restrictions' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, Oxford University Press 2020) 552.
1071 GDPR, Recital 41, states that "[w]here this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to

must be sufficiently clear, foreseeable, and based on one of the exhaustive grounds listed in Art. 23(1) GDPR.[1072] As per Recital 8 GDPR, the reason for the restriction should be comprehensible to the persons to whom it applies. This also involves a clear understanding of how and when the restriction may apply. Restrictions to the data protection principles need to be duly justified by an exceptional situation, respecting the essence of the fundamental rights and freedoms at issue and following a necessity and proportionality test.[1073] The proportionality test should be carried out before introducing in Union or Member State law restrictions and supervisory authorities should be consulted.[1074] According to the ECJ's case law, any legislative measure adopted on the basis of Art. 23(1) GDPR must, in particular, comply with the specific requirements set out in Art. 23(2) GDPR.[1075] In essence, this means that the right of access to information may only be restricted under specific, narrow conditions. Nevertheless, differences may still arise depending on the Member State, particularly given that comparisons with national databases inherently carry a risk of divergent application of the law.

The EDPS suggests that, for instance, where a data subject specifically seeks to exercise a particular right – such as accessing a security flag record – during a particularly sensitive phase of an administrative investigation, the data subject should, where possible, be informed of the reasons for any restriction.[1076] However, if providing this information would undermine the effect of the restriction (i.e., compromise the preliminary objectives of the investigation), disclosure may be withheld. Restrictions may be imposed to protect ongoing investigations, but they must remain necessary and proportionate. To ensure this, the controller should conduct an assessment

persons subject to it, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights."

1072 EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (n 1070) 8 para 17ff.

1073 ibid, 11 para 37; cf 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (European Data Protection Supervisor 2017); cf Moore, 'Article 23 Restrictions' (n 1070) 553.

1074 EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (n 1070) 20, para 86ff.

1075 Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net, French Data Network and Others v Premier ministre and Others* [2020] OJ C 433/3, para 209; cf also Moore, 'Article 23 Restrictions' (n 1070) 552.

1076 EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (n 1070) 14 para 65.

to determine whether informing the data subject of the restriction would prejudice its purpose.[1077] At a later stage – such as after the preliminary phase of an investigation or upon its completion – data subjects should receive a specific data protection notice. It remains possible that, even at this stage, certain rights continue to be restricted, for example, the right of access to information regarding the initiation of an investigation. The data protection notice should explicitly indicate these ongoing restrictions and, where possible, provide a timeframe within which the rights will be fully restored.[1078]

As discussed above, particularly in relation to hits resulting from comparisons with national and international databases, security interests may arise for a Member State or the Union. Such interests can justify restricting access to the relevant information. For instance, this may be the case where a data subject is associated with a terrorist organisation and is consequently listed in a Europol or Interpol database.

The ECtHR, in one case, deals with access to information in regard to migration databases. In Dalea v France, the Court had to deal with a case of a Romanian national who was denied a visa in 1997 for a visit to Germany and the following year for a visit to France. The reason was: he had been reported by the French authorities to the SIS I for the purposes of being refused entry. The applicant applied to the French National Data-Protection Commission (Commission Nationale de l'Informatique et des Libertés (CNIL)), seeking access to his personal data. After exhausting all national remedies, the applicant claimed a violation of Art. 6 and 8 ECHR. With regard to Art. 6 ECHR, the court opined that the applicant's aim had ultimately been to enter the Schengen Area and travel within it. Accordingly, since the proceedings in question were connected with a subject matter falling outside the scope of Art. 6 ECHR, the claim was considered inadmissible.[1079] With regard to Art. 8 ECHR, the Court stated that the applicant had not shown how he had actually suffered as a result of his inability to travel in the Schengen Area. It further opined that the data subject's inability to gain personal access to all the information he had requested, which in particular meant the precise grounds for his inclusion in the SIS I database, could not in itself prove that the interference with

1077 ibid.
1078 ibid, 14, para 67.
1079 *Gheorghe Dalea v France* App no 964/07 (ECtHR 2 February 2010) 3ff.

Art. 8 ECHR was not justified by national security interests.[1080] In the view of the Court, it sufficed that the data subject had been granted access to all the other data concerning him (except for the ground of the inclusion in the SIS I database) and had been informed that considerations relating to state security, defence, and public safety had given rise to the report on the initiative of the Territorial Surveillance Department (Direction de la Surveillance du Territoire).[1081]

Gathering from the above, it can be concluded that access rights can be relatively severely restricted when national security interests are at stake – even if this makes it difficult to defend against the security-related assessment. This is because in the area of entry regulation, states have a broad margin of appreciation. With regard to asylum seekers, however, the margin should be smaller: denying entry might not only violate Art. 8 ECHR, but possibly Art. 3 ECHR. Even in asylum-related cases, access to information rights concerning security-sensitive information may be broadly restricted. In the ECJ's GM v Országos Idegenrendészeti Főigazgatóság case[1082], the Court ruled on the withdrawal of international protection based on national security concerns. It specifically addressed decisions made on the basis of unsubstantiated opinions from national security bodies that determined the individual posed a threat to national security. The case deals with the right to access data primarily in the context of the right to an effective remedy in Art. 47 CFR and will be discussed again in the corresponding chapter. The Court held that when Member States restrict access to information or sources – particularly where disclosure could compromise national security or the safety of the sources – they must ensure that courts competent for international protection decisions can access this information. This access, however, does not extend to the data subject. Furthermore, Member States are required to establish national procedures that safeguard the rights of defence of the individual concerned, which may include granting access to at least part of the relevant data.[1083]

1080 ibid 11: "Elle constate que, si le requérant ne s'est jamais vu offrir la possibilité de combattre le motif précis de cette inscription, il a eu connaissance de toutes les autres données le concernant figurant dans le fichier Schengen, et du fait que le signalement, requis par la DST, se fondait sur des considérations tenant à la sûreté de l'Etat, à la défense et la sécurité publique".

1081 ibid 12.

1082 Case C-159/21 *GM v Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ* [2022] OJ C 424/10.

1083 ibid.

The right of access to data can therefore also be exercised by proxy in national security-related cases. The ECtHR touched on the question of access to data and information in security-related migration cases, in Muhammad and Muhammad v Romania,[1084] where it clarified the procedural safeguards relating to the expulsion of aliens based on national security. The Court elaborated two guiding principles for its assessment: firstly, the more the information available to the alien is limited, the more important it is to introduce safeguards.[1085] Secondly, where the circumstances of a case reveal particularly significant repercussions for the alien's situation, the counterbalancing safeguards must be strengthened accordingly.[1086] The repercussions would certainly be significant, if those data subjects were asylum seekers, in which case safeguards would need to be correspondingly strengthened.

Additionally, as will be discussed in the next chapter, a data subject has the right to be informed – at a minimum – of the essence of the grounds on which a decision based on security information is founded. This right is grounded in the right to an effective remedy.[1087] Data subjects also have to know the identity of the Member State that raised a security-related objection. They ought to know the specific ground for refusal (*in casu* of a visa application) based on that objection.[1088] In the context of Eurodac, this could be interpreted to mean that data subjects must be able to access, at a minimum, information about which database triggered a hit. In the case of an exclusion from international or subsidiary protection, they should also be informed of the specific grounds for that exclusion, along with the essence of the reasons behind it.

1084 *Muhammad and Muhammad v Romania* App no 80982/12 (ECtHR, 15 October 2020).

1085 ibid, para 146. The Court also states in ibid, para 194: "Before those courts, in view of the very limited and general information available to them, the applicants could only base their defence on suppositions and on general aspects of their student life or financial situation (see paragraphs 37-38 above), without being able specifically to challenge an accusation of conduct that allegedly endangered national security. In the Court's view, faced with a situation such as this, the extent of the scrutiny applied by the national courts as to the well-foundedness of the requested expulsion should be all the more comprehensive."

1086 ibid, para 146.

1087 *ZZ v Secretary of State for the Home Department* (n 559).

1088 Joined Cases C-225/19 and C-226/19 *R.N.N.S and KA v Minister van Buitenlandse Zaken* [2020] OJ C 35/10, para 57.

It should be noted that a hit in any of the mentioned databases does not, in itself, establish that an individual poses a definite threat. First, not all information harboured in these databases is correct. For example, there are ongoing discussions about Interpol red notices, which have been misused by authoritarian regimes.[1089] Also, data comparisons with national databases have been criticised by the EDPS, because they add the issue of a lack of harmonisation and uneven or arbitrary labelling of someone as a security risk.[1090]

In any case, it is argued here that these minimum criteria for access to personal data apply only to the security flag information, not to the information on which the recording of the security flag in Eurodac is based. In other words, as explained above, this study makes a distinction between potential intelligence information (hit after a data match during the security-check under the Screening Regulation) and police information (the question of whether a person is violent, unlawfully armed or there are clear indications that the person is involved in a criminal offence according to the Eurodac Regulation).

The assessment required to determine whether one of the three criteria justifying the addition of a security flag in Eurodac has been met[1091] must be made accessible to the data subjects.[1092] Such an assessment is not based on intelligence information, but in most cases on police information. Recital 8 Eurodac Regulation states that when assessing whether a person is violent, it is necessary that a Member State determines whether the person has displayed behaviour that results in physical harm to other persons that would amount to a criminal offence under national law. Whether a person is unlawfully armed, or there are clear indications that the person is involved in a criminal offence, will also (in most cases) be deduced from police

1089 Serdar San, 'Transnational Policing between National Political Regimes and Human Rights Norms: The Case of the Interpol Red Notice System' (2022) 26 Theoretical Criminology 601.

1090 D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 2.

1091 See for more details on such assessments chapter: The Right to an Effective Remedy.

1092 It could, however, be argued, that this data is not personal data according to *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), paras 45 and 46, and *Peter Nowak v Data Protection Commissioner* (n 1033), para 56, or under the new EJC jurisprudence P *OC v European Commission* (n 1039); *Patrick Breyer v Bundesrepublik Deutschland* (n 1040); *SRB v European Data Protection Supervisor* (n 1038).

information. Such accusations and the evidence supporting them would have to be accessible to the accused in a criminal procedure.[1093] It should therefore be accessible under the Eurodac Regulation. After all, the right of access is necessary, *inter alia*, to enable the data subject to obtain the rectification, erasure or blocking of their data.[1094] It should be noted that consequence of a security flag being erased in Eurodac would not lead to the data subject concerned being cleared in any other database, for example an Interopl or national security database.

It should also be taken into account that security flags based on an entry in another database carry the risk of duplicating information, which carries data protection risks.[1095] For instance, if the record in the underlying database, e.g. an Interopl databse, is deleted, the security flag in Eurodac may remain: security flags are only deleted when the Member State of origin decides that the threat no longer applies and has consulted any other Member State having registered a data set of the same data subject.[1096] While this process should ideally align with the deletion of the data subject's record in the database that produced the hit, Member States are not required to follow the assessment of another EU agency or Member State.

In conclusion, limitations on access to personal data appear more readily justifiable with respect to hits generated during the security check under the Screening Regulation. By contrast, restricting access in relation to the three conditions for entering a security flag in Eurodac (violent, unlawfully armed, or indications of involvement in a criminal offence) would require a substantially stronger and more carefully articulated justification.

1093 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings [2012] OJ L142/1, Art 6 and 7; according to *Rowe and Davis v the United Kingdom* ECHR 2000-II, para 60, the right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party.

1094 *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), para 44; *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857), paras 49 and 51.

1095 D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 3.

1096 Eurodac Regulation 2024, Art 17(4).

ccc) *Logs and Records on Recipients of Data*

The data subject must have access to whom specifically data have been disclosed. The right to access information about recipients of personal data is contained in Art. 43 in conjunction with Art. 42(1)(d) Eurodac Regulation and has been confirmed by the ECJ.[1097] It serves the important function of giving the data subject the chance to understand how their personal data are being processed and what the consequences of such processing are.[1098] This right is more specific than the right to information, wherein only potential data recipients have to be named.[1099] However, a distinctive feature of Eurodac data (or all data in interoperable databases) is that data are not only shared but more often directly accessed by other authorities. According to Art. 4(9) GDPR, a 'recipient' is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed. According to Art. 4(2) GDPR, disclosure means "transmission, dissemination or otherwise making available of data". If an authority gains access to Eurodac data, even if it is just in read-only format, these data have been disclosed to them, which makes them recipients in the sense of the Union data protection law.

As discussed in the last chapter, Art. 4(9) GDPR includes an exception to the broad definition of recipients. It states that public authorities receiving personal data in the context of a specific inquiry, in accordance with Union or Member State law, should not be considered recipients. It follows from that definition of recipients that possible access to Eurodac data by Europol and national law enforcement authorities would probably not have to be communicated to the data subjects if this were not expressly provided for in the Eurodac Regulation.[1100] The supervisory authority as a recipient must not be declared to the data subjects, since it only grants access in the context of specific investigations or inquiries. Other authorities, such as national visa, immigration or asylum authorities of Member States, third

1097 *RW v Österreichische Post AG* (n 857), para 25; cf also *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857).

1098 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 9 para 10.

1099 *RW v Österreichische Post AG* (n 857), para 25; Dix, 'Article 15 - Right of Access by the Data Subject' (n 662), para 14.

1100 Eurodac Regulation 2024, Art 42(1)(b).

countries, and eu-LISA may not be covered by the exception in Art. 4(9) GDPR.[1101]

Access to Eurodac data is documented in the form of logs or records. eu-LISA must keep records of all data processing operations within Eurodac.[1102] These records may be used only for the data protection monitoring of the admissibility of data processing and to ensure data security. Data protection monitoring is exercised by national data protection authorities and the EDPS; data security lies with eu-LISA and national authorities. Data subjects might thus not be provided access to such records.[1103]
eu-LISA also must keep such records for the purposes of interoperability with ETIAS. These records shall additionally show the hits triggered while carrying out the automated processing.[1104] For the purpose of access to Eurodac by visa authorities, Member States and eu-LISA keep records of each data processing operation carried out within Eurodac and the VIS.[1105] The Eurodac Regulation does not clarify who might have access to such records. Since a hit triggered with one's personal data can be qualified as personal data too, at least records of hits should be accessible to data subjects.

Moreover, Member States and Europol have to log or document all data processing operations resulting from requests for comparison with Eurodac data for the purposes of the prevention, detection, or investigation of serious criminal offences.[1106] These records are used to check the admissibility of requests, monitor the lawfulness of data processing, ensure data integrity,

1101 See chapter: The Right to Information.

1102 Eurodac Regulation 2024, Art 41(1): "Eu-LISA shall keep records of all data processing operations within Eurodac. These records shall show the purpose, date and time of access, the data transmitted, the data used for interrogation and the name of both the unit entering or retrieving the data and the persons responsible." Although the records themselves are made by the Member States according to ibid, Art 41(5).

1103 Also, the eu-LISA Regulation does not contain an access right (Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice [2018] OJ L295/99 (eu-LISA Regulation)). However, the Regulation on the processing of personal data by the Union institutions, bodies, offices and agencies applies to ibid, Art 35(1) which contains a right to access by the data subject in ibid, Art 17.

1104 Eurodac Regulation 2024, Art 41(2).

1105 ibid, Art 41(3) in conjunction with Amendment to the VIS Regulation 2021, Art 34.

1106 Eurodac Regulation 2024, Art 51(1).

and support security and self-monitoring efforts.[1107] The provision contains a list of information which has to be shown in all logs or documentation, including the purpose for the request, the offence concerned, the national file number, name of the authority that requested access, and those who ordered and carried it out as well as the data used for comparison.[1108] Logs that contain personal data can be used for monitoring the lawfulness of data processing and data security and integrity, which, as stated above, is exercised by national data protection authorities, the EDPS or eu-LISA. For monitoring and evaluation, only non-personal data can also be used.[1109] Here, too, it seems that data subjects might not have access to such records. Records and logs are also not among the information that has to be stored in Eurodac according to Art. 17 Eurodac Regulation. This might indicate that data subjects can't access them.[1110] It seems that data subjects do not have access to records and logs.

According to Art. 47(4) Eurodac Regulation, Eurodac, the designated and verifying authorities, and Europol also shall keep records of searches in the context of law enforcement purposes. The records are used for permitting the national data protection authorities and the EDPS to monitor the compliance of data processing with Union data protection rules and for preparing annual reports.[1111] Other than for such purposes, the records of the searches shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.[1112]

It seems that data subjects might be able to access these records. Access by a data subject could fall under 'other purposes', since they are neither a national data protection authority nor the EDPS. Records of the searches are, for access purposes, erased after one month in national and Europol files, but not, so it seems, in Eurodac. Since data subjects have access to "data relating to him or her recorded in Eurodac", they should be able to access these records of searches in the law enforcement context concerning their personal data.

1107 ibid.
1108 ibid, Art 51(2).
1109 ibid, Art 51(3).
1110 cf Eurodac Regulation 2024, Art 43(1).
1111 ibid, Art 47(4).
1112 ibid, Art 47(4). Data subjects are not informed before the logs are deleted.

The distinction between the logs documenting searches under Art. 47(4) Eurodac Regulation and those documenting data-processing operations resulting from requests for comparison under Art. 51 is not entirely clear. The former appear, at least in principle, to be accessible to data subjects, whereas the latter are not. Yet a search is itself a processing operation, insofar as it entails the comparison of the data entered into the search interface with the data stored in the database. Whether, in practice, access to law-enforcement searches will be granted therefore remains uncertain.
Although data subjects must be informed that law-enforcement authorities may access their data, it can be argued that – aside from this specific obligation – these authorities are not to be regarded as "recipients", which could preclude any right of access to related logs or records. In any event, access to logs and records would in all cases be subject to the restrictions permitted under Art. 23 GDPR. Moreover, the privacy rights of the individuals whose identities appear in logs of processing operations or requests must also be safeguarded.

In its J.M. judgment, the ECJ ruled, with regard to logs, specifying consultation operations carried out on a data subject's personal data and concerning the dates and purposes of those operations, that these logs constitute personal data of the data subjects.[1113] Data subjects thus have a right to obtain these logs. However, the right does not extend to the information relating to the identity of the employees of the controller who carried out the operations, unless that information is essential in order to enable the data subject concerned effectively to exercise its rights under the GDPR and provided that the rights and freedoms of those employees are taken into account.[1114] This judgment indicates that, even though the Eurodac Regulation does not guarantee access to logs (at least not in all cases), such access should nonetheless be made available to data subjects. This position is further reinforced by the subsequent case law.

In its judgment, RW v Österreichische Post AG, the ECJ reaffirmed previous rulings and stated that the exercise of the right of access must enable the data subject to verify not only the accuracy of their data but also the lawfulness of its processing.[1115] Specifically, the data subject should be able

1113 Case C-579/21 *J.M.* [2023], para. 90. The Finnish Assistant Data Protection Supervisor considered these logs to be personal data of the employees who processed the data (para. 25).

1114 ibid.

1115 *RW v Österreichische Post AG* (n 857), para 37, referring to, by analogy, *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en*

to confirm that their data have been disclosed to authorised recipients.[1116] The Court finds the right of access particularly necessary in order to enable the data subject to exercise their right to rectification and erasure.[1117] The information provided to the data subject pursuant to the right of access must be as precise as possible. The right of access specifically allows the data subject to obtain information from the controller about the specific recipients to whom their data have been or will be disclosed. Alternatively, the data subject can choose to request information about the categories of recipients instead.[1118] The Court adds that the right to access personal data is not absolute; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[1119] Therefore, it may be accepted that, "in specific circumstances", it is not possible to provide information about specific recipients, in particular where they are not yet known.[1120]

In a previous decision, Rijkeboer, the ECJ ruled that access to information about recipients can be restricted if the obligation to maintain this information for an extended period imposes an "excessive burden" on the controller.[1121] This can be the case, e.g., because of high frequency of disclosure to a more restricted number of recipients.[1122] The Court opined that limiting access to recipients' information, while basic data are stored for a much longer period, does not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller.[1123]

Asiel v M. and S. (n 558), para 44 and *Peter Nowak v Data Protection Commissioner* (n 1033), para 57. *F.F. v Österreichische Datenschutzbehörde and CRIF GmbH* (n 957), para 34.

1116 *RW v Österreichische Post AG* (n 857), para 37, referring to, by analogy, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857), para 49.

1117 *RW v Österreichische Post AG* (n 857), para 38, referring to, by analogy, *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), para 44 and *Peter Nowak v Data Protection Commissioner* (n 1033), para 57.

1118 *RW v Österreichische Post AG* (n 857), para 43.

1119 ibid, para 47, referring to, by analogy, Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] OJ C 297/4, para 172.

1120 *RW v Österreichische Post AG* (n 857), para 48.

1121 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857).

1122 ibid, paras 59 and 66.

1123 ibid, para 66.

As explained above, under the Eurodac Regulation (and, as will be shown later, under the Interoperability Regulation), data subjects have only limited access to information concerning the recipients of their personal data. In light of the relevant case-law, it is questionable whether such a restrictive approach is sustainable. It does not appear that "special circumstances" exist that would justify these limitations on the right of access to personal data, particularly with respect to information on data recipients. Since logs are produced and kept at various levels anyway, it would also not be an "excessive burden" for the Member States to make them available.

ddd) *Reasons for Rejection*

Art. 43(8) Eurodac Regulation states that "whenever a person requests access [...], the competent authority shall keep a record in the form of a written document that such a request was made and how it was addressed, and shall make that document available to the national supervisory authorities without delay." The Eurodac Regulation does not contain a provision stating, in case the access request is denied, that the grounds for the decision should be communicated to the data subject. This is provided only for rectification and erasure requests[1124] and therefore differs from the SIS II and the new SIS Regulations (referred to here as SIS III Regulations[1125]) as well as the VIS Regulation.[1126] The absence of a requirement in the

1124 Eurodac Regulation 2024, Art 43(5).

1125 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) [2006] OJ L381/4 (SIS II Regulation), Art 41(6); Council Decision 2007/533/JHA of 12 June 2007 on the Establishment, Operation and Use of the Second Generation Schengen Information System [2007] OJ L205/63 (SIS II Decision), Art 58(6); Proposal for a Regulation of the European Parliament and of the Council on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Police Cooperation and Judicial Cooperation in Criminal Matters as Regards the Entry of Alerts by Europol [2016] COM(2016)883 (SIS III Police Proposal), Art 65(6); Proposal for a Regulation of the European Parliament and of the Council on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Border Checks [2016] COM(2016)882 (SIS III Borders Proposal), Art 47(5); Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the Use of the Schengen Information System (SIS) for the Return of Illegally Staying Third-Country Nationals [2018] OJ L312/1 (SIS III Return Regulation), Art 13.

1126 VIS Regulation 2008, Art 38(7).

Eurodac Regulation to provide reasons for rejecting an access request does not negate the data subject's right to an explanation. The right to reasons is encompassed in the right to a fair procedure.[1127] In the event that an application for access is rejected or only partially approved, grounds for the decision must also be provided and accessible under the Eurodac Regulation.

eee) *Information Regarding Sharing of Data*

Another question is whether information regarding the transfer of data to a third party is accessible. It is not clear from Art. 49 and 50 Eurodac Regulation whether the sharing of data with third parties leads to an entry in Eurodac.[1128] There are three situations in which data sharing is possible under the Eurodac Regulation. First, data following a hit obtained for law enforcement purposes can be shared with a third country if there is no "real risk" that as a result of such transfer the data subject may be subjected to a violation of their fundamental rights.[1129] There are no rules in the Eurodac Regulation regarding how the assessment of such a risk is conducted. As mentioned in the last chapter, oftentimes, no data protection standards with regard to third countries seem to be in place.[1130] Any assessment should be stored in order for a Member State to prove their action was lawful, if

1127 TFEU, Art 296, imposes a duty to give reasons in relation to all legal acts; cf also CFR, Art 41 and Art 47; according to Craig, 'Article 41 - Right to Good Administration' (n 880), para. 41.17: It is possible that Article 41 might be interpreted more broadly than Article 296 TFEU, since the word 'administration' might be taken to include national administration, thereby requiring it to provide reasons when it acts in the scope of EU law, as would be the case when a national agency is part of a scheme of shared administration. An obligation to give reasons by national administration has in any event been imposed in particular cases, where it is regarded as necessary to safeguard other important principles of EU law (cf e.g., Case 222/86 *Unectef v Georges Heylens and others* [1987] ECR 4097, para 15); also Debbie Sayers, 'Article 47 – Right to an Effective Remedy and to a Fair Trial' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Bloomsbury Publishing 2022), para 47.392ff.

1128 Unlike Eurodac, the GDPR explicitly regulates this issue. According to GDPR, Art 15(2), where personal data are transferred to a third country or to an international organisation, information on safeguards pursuant to Art. 46 can be accessed by the data subject; see also EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 2.

1129 2016 Eurodac Proposal, Art 49(2).

1130 See chapter: The Right to Information.

liability questions arise.[1131] Such an assessment, it could be argued, might be mere "information about the assessment and application by the competent authority of the law to the applicant's situation" and therefore not personal data.[1132] Since it informs or constitutes the final decision that leads to the data transfer, it must be distinguished from a draft decision.[1133] This final decision serves as the basis for assessing any legal remedy against it.[1134] Furthermore, the assessment also entails the recipient of data (the third country), which is information that has to be accessible.[1135] The assessment therefore qualifies as personal data and should be available to data subjects, even if it is not stored within Eurodac. Such information is also not, as such, security-sensitive and no ground for restriction according to Art. 23 GDPR applies.

Even if access to such information is granted, as discussed in the last chapter, in practice, data subjects might not be informed about a data transfer (although this study argues that they should be). Then, chances are high that they will not ask to access information, such as the risk assessment, and will not have a chance to challenge it before (or even after) such data are transferred.

The second situation, in which Eurodac data can be transferred to third parties, is for return purposes.[1136] The conditions for such a transfer are, as mentioned in the last chapter, first, that the Member State of origin agrees. Second, the data are transferred or made available solely to identify and issue an identification or travel document to an illegally staying third-country national for return purposes. The third-country national concerned must be informed that their personal data may be shared with the authorities of a third country.[1137] As previously mentioned, the Proposal

1131 Eurodac Regulation 2024, Art 60.

1132 *Y.S. v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M. and S.* (n 558), para 40.

1133 ibid.

1134 cf Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017], Opinion of AG Kokott, para 63: "Precisely because of that close link between the examination script and any corrections made on it, the latter also are personal data of the examination candidate pursuant to the Data Protection Directive 95/46/EC, Art 2(a)."

1135 Eurodac Regulation 2024, Art 43(1) in conjunction with ibid, Art 42(1)(d), *RW v Österreichische Post AG* (n 857) and *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857).

1136 Eurodac Regulation 2024, Art 49.

1137 ibid, Art 50(1) and (3).

for a Eurodac Regulation from 2016 stated that the receiving country must explicitly agree to use the data only for the purpose for which it was provided. Additionally, it required that the data be deleted when it is no longer justified to keep them. However, these provisions were not included in the current law.[1138] The transfer of data under the Eurodac Regulation is not tied to the condition that the receiving state provides a certain level of data protection.[1139] In many cases, data transfers will be conducted based on the derogation provision in Art. 49(1)(b) GDPR.[1140]

To secure at least some degree of data protection, the Member State's agreement – required as the first condition for a data transfer – must be accompanied by a substantive assessment. Where no adequacy decision under Art. 45 GDPR exists, and no appropriate safeguards under Art. 46 GDPR can be ensured, this assessment should include a weighing of the Member State's important public interests against the data protection risks for the data subject. Such agreements could then be monitored by the national independent supervisory authority.[1141] An agreement, like the assessment, can be qualified as personal data and should be accessible.

As has been argued in the last chapter, data subjects should be informed of a transfer not only when providing biometric data, but also before the transfer is conducted. If this is not the case, the data subject will not, in all likelihood, request access before such a data transfer and accordingly not be able to challenge it.

Finally, Eurodac data can also be shared according to GDPR rules.[1142] Access and information rights are, in these cases, governed by the GDPR.

fff) *Anonymised Data*

One of the objectives of the Eurodac reform was to gather more statistics to forecast border crossings and migration patterns. However, academics and practitioners in the asylum field have raised concerns about these data. They warn that it could be used to interdict, curtail, and prevent access to international protection procedures. This would breach the right to seek

1138 2016 Eurodac Proposal, Art 38(1).
1139 Eurodac Regulation 2024, Art 49 and 50.
1140 See chapter: The Right to Information.
1141 cf Eurodac Regulation 2024, Recital 85.
1142 2016 Eurodac Proposal, Art 37(4).

asylum and the principle of non-refoulement. Additionally, such actions may compel people to take more dangerous routes to Europe.[1143]

Data in Eurodac are stored for a ten-,[1144] five-,[1145] three-[1146] or one-year[1147] period from the transmission date.[1148] After these time periods, data have to be deleted. They are no longer at the disposal of a controller and thus can't be accessed anymore.[1149] Still, they might be used in an anonymised form for statistics and reporting.[1150] Anonymised data do not count as personal data anymore,[1151] other than personal data which have undergone pseudonymisation.[1152] Anonymised data in the form of statistics can to some degree still be accessed by data subjects. Some of them are made public, other parts might be accessible with freedom of information requests.[1153] Since they are not considered personal data anymore, access cannot be requested based on Art. 43 Eurodac Regulation.

Finally, under Art. 4(2) of the Eurodac Regulation, eu-LISA may use real personal data from the Eurodac production system for specific testing purposes. At present, there appears to be no way for data subjects to know whether their data have been used for such testing or to access any corresponding information.

1143 Letter to Members of the European Parliament, Abdullah Elbi and others, 'Legal Experts Representing and Defending Migrants' Rights Call on EU Legislators to Reject the EURODAC Reform' (4 April 2024) 1; Chloé Berthélémy, 'Eurodac Database Repurposed to Surveil Migrants' (*edri.org*, 10 March 2021) <https://edri.org/our-work/eurodac-database-repurposed-to-surveil-migrants/>.

1144 Eurodac Regulation 2024, Art 29(1).

1145 ibid, Art 29(3), (5 - 8).

1146 ibid, Art 29(4) in conjunction with ibid, Art 18(2)(b) or (c).

1147 Eurodac Regulation 2024, Art 29(9) in conjunction with ibid, Art 26(1).

1148 Eurodac Regulation 2024, Art 29(3), (5-8).

1149 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 18 para 38.

1150 Eurodac Regulation 2024, Art 12(3).

1151 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 3.

1152 ibid 4; cf also *SRB v European Data Protection Supervisor* (n 1038), paras 99, 102 and 104ff.

1153 eu-LISA Regulation, Art 34, underlines that the Access to Documents Regulation (Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding Public Access to European Parliament, Council and Commission Documents [2001] OJ L145/43 (Access to Documents Regulation)) shall apply to the Agency in its entirety, with particular regard to the EU legal acts governing the development, establishment, operation and use of large-scale IT-systems.

bb) Under the Interoperability Regulation

As already discussed, the Interoperability Regulations refer to the GDPR regarding access requests. The only provision in the Interoperability Regulations addressing the content to be communicated to the data subject is Art. 48(11). It states that, "[t]his Article is without prejudice to any limitations and restrictions to the rights set out in this Article pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680." The Interoperability Regulations do not provide further information on what data must be accessible. Therefore, Art. 12, Art. 14 and Art. 15 GDPR are applicable.

aaa) *Data in the CIR and sBMS*

The right of access in the Interoperability Regulation only applies to personal data in the MID,[1154] especially whenever the MID created a red link, as well as whenever the data subject concerned is being informed about this and will need to verify their identity.[1155]
One might ask whether data in the CIR or in the sBMS should also be accessible. The CIR is a database of its own.[1156] It contains some personal

1154 Interoperability Regulation - Judicial Cooperation, Art 48.
1155 Interoperability Regulation - Judicial Cooperation, Art 49(2).
1156 EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646) 11 para 28; Art. 29 WP 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 4; more critically: Gutheil, Liger and Eager, 'Interoperability of Justice and Home Affairs Information Systems' (n 71) 63ff: "Critically, the proposals are lacking clarity as to how the CIR will function technically. The proposal explicitly states that the CIR is not a new database, but rather a shared technical component between all the systems that would store and search the biographical data across all the central systems. However, the use of terms such as 'store' and 'storage' throughout the proposal and the accompanying impact assessment implies the creation of a new database that will store the data of all third-country nationals (Proposal for a Regulation of the European Parliament and of the Council on Establishing a Framework for Interoperability between EU Information Systems (Borders and Visas) [2017] COM(2017)793 (Proposal for an Interoperability Regulation 2017 - Borders) 29). In a section on the compatibility with previous initiatives with regard to how the solutions were developed, the proposal states, '[i]t became clear afterwards a distinction had to be made between the CIR as the database of identities and a new component that identifies multiple

data that are not stored in the underlying databases, such as Eurodac: a hit indicating that data on a person are stored in the CIR constitutes personal data,[1157] as do the coloured MID links between identities.[1158] Some may argue that because the sBMS does not process personal data and merely stores templates of biometrics, it cannot be considered to be a database. However, this study follows the opinion that data stored in the sBMS are in fact biometric data in themselves. Hence, the sBMS stores personal data and has to be qualified as a database.[1159] Accordingly, a right of access to

---

identities linked to a same biometric identifier (MID)'. This may have been simply a semantic error, but confusion could be avoided if there was greater clarity on the technical functionality of the CIR. What is clear is that the CIR will have 'database-like' functionality that will permit querying of the identity data of all third-country nationals within the underlying systems."

1157 Art. 29 WP, 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 13.

1158 Gutheil, Liger and Eager, 'Interoperability of Justice and Home Affairs Information Systems' (n 71) 65.

1159 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 7ff: "According to the Commission's Impact Assessment, the sBMS would not handle any new data and it would not modify any existing end-user access rights. It would contain "non-sensitive" biometric templates without any biographical data. […]" However, WP 29 takes the view that biometric templates cannot be regarded as non-sensitive data: "They may contain a more limited amount of personal information than the biometric data themselves and in a coded form, but that extract serves as a preprocessed format for matching and is capable of providing unique identification in an automated matching process (cf Art. 29 WP, 'Opinion 3/2012 on Developments in Biometric Technologies' (2012) 00720/12/EN WP 193). The special power of biometric data is their capacity to serve as a universal identifier allowing information about the same person to be linked across different information sources (referring to Anne Carblanc, 'Human Rights, Identity and Anonymity: Digital Identity and Its Management in e-Society' in Emilio Mordini and Manfred Green (eds), *Identity, security and democracy: the wider social and ethical implications of automated systems for human identification* (2009) 11), This is exactly the intended use of the biometric templates here and therefore a biometric template has to be qualified as biometric data […]."
See for a more comprehensive analysis Gutheil, Liger and Eager, 'Interoperability of Justice and Home Affairs Information Systems' (n 71); cf also Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (n 35) 94 - 100; European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a Research Project Funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' (2011) 4 and

these databases exists in accordance with Art. 15 GDPR. Particularly with regard to the CIR, access should be granted because it stores data that are not stored in other databases, as was mentioned above. Furthermore, data subjects may not be aware of which of the several interoperable databases contain their personal data. From an access to justice perspective, this makes it necessary to grant access to the CIR in order for the data subject to be able to know which information systems harbour personal data about them. Whether an access request to the CIR based on the GDPR will be granted in practice remains to be seen.

bbb) *Data in the MID and Automated Processing*

As mentioned above, the right of access in the Interoperability Regulation applies to personal data in the MID.[1160] The MID stores identity confirmation files. These files contain links between data in the EU information systems included in the CIR and SIS. They also include a reference to the EU information systems where the linked data are held. Each file has a single identification number that allows retrieval of the linked data from the corresponding EU information systems. Additionally, the files specify the authority responsible for the manual verification of different identities and the date of creation or any updates to the link.[1161] This information may be considered personal data or a recipient (in the case of the case of the authority responsible for the manual verification), which is accessible to data subjects under the Interoperability Regulation.

The EDPS has noted how the functioning of the MID allowing the detection of the use of multiple identities by third-country nationals qualifies as

ibid 5; Bilgesu Sumer, 'When Do the Images of Biometric Characteristics Qualify as Special Categories of Data under the GDPR?: A Systemic Approach to Biometric Data Processing', *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)* (2022); the IDEMIA group, who built the sBMS writes on their homepage: "By 2022, the sBMS will be one of the largest biometric systems in the world, integrating a database of over 400 million third-country nationals with their fingerprints and facial images" ('IDEMIA and Sopra Steria Chosen by Eu-LISA to Build the New Shared Biometric Matching System (sBMS) for Border Protection of the Schengen Area' (*Idemia Group*, 6 April 2020) <https://www.idemia.com/press-release/idemia-and-sopra-steria-chosen-eu-lisa-build-new-shared-biometric-matching-system-sbms-border-protection-schengen-area-2020-06-04>).

1160 Interoperability regulation - Judicial Cooperation, Art 49(2).

1161 ibid, Art 25 in conjunction with ibid, Art 34.

automated decision-making.[1162] It also notes the difficulty for individuals to access the reasoning underlying a decision detecting multiple identity use, which poses particular transparency challenges.[1163] Data protection rules traditionally grant individuals a high level of protection in such circumstances, given the lack of human intervention and potential intrusiveness into the private sphere. This includes the right to access information about the existence of automated decision-making, including profiling. In these cases, individuals are entitled to receive meaningful information about the logic involved. They should also be informed about the significance of the processing and the anticipated consequences for the data subject.[1164] Data subjects have to be able to access information on the functioning of the MID. It can be argued that the MID algorithm (which is the logic involved) will have to be made available to the data subject – or at least, meaningful information on how it works. As seen above, such information should be displayed in a form that is understandable for the data subject.[1165]

ccc) *Logs Documenting Access*

The next question is whether a data subject should have the right to be able to comprehend who accessed their data and how they were processed and used. Logs of all data processing operations in the MID,[1166] the sBMS,[1167] the ESP,[1168] and the CIR[1169] are stored by eu-LISA. They are not accessible

1162 EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646) 21 para 86.
1163 ibid 21 para 87ff; Curtin and Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 64.
1164 Interoperability Regulation - Judicial Cooperation, Art 15(1)(h).
1165 cf *BU v Federal Republic of Germany* (n 1011).
1166 Interoperability Regulation - Judicial Cooperation, Art 36.
1167 ibid, Art 16(1).
1168 ibid, Art 10(1).
1169 ibid, Art 25(1).

based on the Interoperability Regulation.[1170] The same goes for logs kept by Europol documenting access to the CIR.[1171]

Logs of processing operations in the MID and CIR are also stored at the national level.[1172] The logs documenting the very wide access to the CIR for identification purposes by police authorities[1173] specifically have to entail the purpose of access, the national file reference, and the unique user identity of the official who carried out the query and of the official who ordered the query.[1174] For data subjects, access rights to these logs would be guided by the GDPR. This stipulates that data subjects must be informed about the recipients or categories of recipients to whom their personal data have been or will be disclosed.[1175] As was discussed above, law enforcement authorities may not be considered recipients if they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law.[1176] Also, the Interoperability Regulation states that the logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, as well as for ensuring data security and integrity.[1177] They are erased one year after their creation, unless they are required for monitoring procedures that have already begun.[1178] These tasks could to some degree be fulfilled by data subjects themselves. However, the Interoperability Regulation does not

1170 The eu-LISA Regulation does not contain an access right (eu-LISA Regulation). However, the Regulation on the processing of personal data by the Union institutions, bodies, offices and agencies applies to ibid, Art 35(1), which contains a right to access by the data subject in its Art 17.

1171 Interoperability Regulation - Judicial Cooperation, Art 25(6). An access request could be based on the Europol Regulation.

1172 Interoperability Regulation - Judicial Cooperation, Art 24(5) and 36(2); cf EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646) 29 paras 133ff and ibid 29 para 136: "The EDPS therefore recommends to store the logs of the ESP and the shared BMS also at national level, as are the logs of the CIR (Article 24(5)) and the MID (Article 36(2))."

1173 Interoperability Regulation - Judicial Cooperation, Art 20.

1174 ibid, Art 24(5).

1175 GDPR, Art 15(1); *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857), paras 68 and 69; see also *RW v Österreichische Post AG* (n 857), para 26, in which Court stated that the EU legislature did not intend to reduce the level of protection under the GDPR as compared to the Data Protection Directive 95/46, which means that earlier case law (i.e., Rijkeboer) can be applied and confirmed that data recipients have to be disclosed (para. 43).

1176 GDPR, Art 4(9).

1177 Interoperability Regulation - Judicial Cooperation, Art 24(7) and 36(3).

1178 ibid, Art 24(7) and 36(3).

provide for this. It must be assumed that data subjects do not have access to logs with information regarding the recipients of their personal data.

The case law discussed in the chapter on access to information about recipients under the Eurodac Regulation should also be considered in the context of interoperability. It remains questionable whether the Interoperability Regulation provides sufficiently detailed access to information about who accessed Eurodac data within the interoperability framework.[1179] The interoperability project faced criticism during the legislative process, particularly regarding the extent to which transparency in data processing would be maintained.[1180] Related to this is the question of the subject status and the dignity of the data subjects concerned.[1181] Transparency is compromised if data recipients and the processing of personal data cannot be traced by the data subject. The interoperability system is highly complex, and by limiting access to certain data in the MID, the EU has made it nearly impossible for data subjects to understand how their information is used. By restricting data subjects' rights despite the aforementioned case law, interoperability also creates an unjustified disparity between EU (and Schengen/Dublin-associated) citizens and third-country nationals.

ddd) *Statistical Data*

Finally, as mentioned, the Central Repository for Reporting and Statistics (CRRS) forms part of the interoperability system. It was established to support the objectives of the information systems and "provide cross-system

1179 cf FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674) 34; also *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (n 1119); *RW v Österreichische Post AG* (n 857); *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (n 857).

1180 cf FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71); EDPS, in its 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646); Evelien Brouwer, 'Interoperability of Databases and Interstate Trust: A Perilous Combination for Fundamental Rights' (*Verfassungsblog*, 25 May 2019) <https://verfassungsblog.de/interoperability-of-databases-and-interstate-trust-a-perilous-combination-for-fundamental-rights/> Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55); Hartmut, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (n 73).

1181 See chapter: Access to Justice.

statistical data and analytical reporting for policy, operational and data quality purposes."[1182] It should be noted that AI techniques will be deployed in the CRRS, which may provide it, e.g., with "automated mechanisms to predict and discover potential risks," according to a study by private companies and commissioned by the EU.[1183] As was discussed in the last section, anonymised data do not count as personal data.[1184] Anonymised data can therefore only be accessed in so far as the statistics created by them are available to the public. However, according to the EDPS, data stored in the CRRS may nevertheless lead to the identification of individuals in certain cases.[1185] Contrary to the wording in Art. 62 (2) Interoperability Regulation, the supervisory says, the combination of nationality, gender, and year of birth of the person could lead to individual identification.[1186] 'Personal data' in the sense of the GDPR means "any information relating to an identified or identifiable natural person ('data subject') [...]."[1187] Hence, if personal data in the sense of the GDPR are used in the CRRS, data subjects will have to be able to access them. Furthermore, they also should be informed who accessed their data for the purpose of reporting and statistics, since the "duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA", which can access such data for this purpose, are then to be considered recipients of personal data.[1188]

1182 Interoperability Regulation - Judicial Cooperation, Art 39(1).

1183 'LISA/2019/OP/01' Transversal Engineering Framework (TEF) (*Unisys Belgium, Unisys Luxembourg and Wavestone*, November 2022). The report is clear in that it is "a research document and the outcome does not indicate that the AI Solutions will be utilised in the manner suggested and described in the Study." However, the report also says that the system's ability "to learn based on data inputs and/or outputs" should "extend beyond the specific objectives of this project"; for more see Jones, Lanneau 'Automating Authority: Artificial intelligence in European police and border regimes' (n 231).

1184 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553) 3.

1185 D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 5; EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), para 100.

1186 D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 5; EDPS 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), para 100.

1187 GDPR, Art 4(1).

1188 ibid, Art 15(1)(c).

cc) Conclusions

The previous section shows that much is still unclear with regard to the right of access to data in Eurodac and the interoperability systems, especially concerning important aspects such as the scope of accessible data in relation to hits and the security flag. It has also been shown that Eurodac and the Interoperability Regulations only provide for rather limited access to personal data. For example, neither regulation offers any way of actually tracing who has been given access to the Eurodac data and what they have done with it. Even with regard to the automated decision-making in the MID, the Interoperability Regulation itself does not ensure that a data subject has access to information on the technology and logic involved. Understanding the already highly complex data processing procedures of interoperable information systems is all the more difficult when data subjects do not receive sufficient information – even if they take it upon themselves to submit a request for access.

It should be added here that the EU is endeavouring to share more data with ever more authorities. In a document by the Council of the European Union in 2022 on "[i]mproving the transmission of information between administrations in the follow-up of persons representing a terrorist threat", it was stated that, in order to better adjust administrative or judicial measures, it would be useful for the "competent services to be able – in addition to the information which will be indicated in the near future in the revised Eurodac system – to identify in which Member State an application for international protection has been lodged by a migrant and to be able to obtain basic information on the progress status of this procedure. […] The status of any appeals lodged by an individual whose application has been rejected, which generally have the effect of suspending removal orders, would also be useful information."[1189] Especially in cases where data subjects actually and demonstrably jeopardise the security situation of a Member State or the Union or pose a terrorist threat, a Europe-wide exchange of data may be able to prevent crime. However, the general thrust of using all migration-related data for security purposes also leads to a restriction of data protection for third-country nationals, which is visible in the Eurodac and Interoperability Regulations. This applies equally to

1189 6247/22 from Presidency, Council of the European Union, 'Improving the Transmission of Information between Administrations in the Follow-up of Persons Representing a Terrorist Threat' (22 February 2022).

data subjects who have not (or not yet) been involved in any criminal proceedings and to those with a prior criminal history.

3. Case Law: Access to Personal Data and Information in National Case Law

In contrast to the right to information, there is a substantial body of case law from European courts concerning the right of access to personal data and information. It thus seems clear that this right is justiciable. The refusal of access to data and information can, in principle, be contested. However, it is worth noting that a 2025 study on access to SIS II data found that certain EU Member States, in particular Italy, systematically reject access requests.[1190] However, this practice appears to be unlawful in light of the ECJ case Ligue des droits humains, which requires an individual assessment of access requests and a justification in the event of a refusal.[1191] The main unresolved issue regarding Eurodac data is thus how broadly the right of access to personal data and information will be interpreted in practice.[1192] This is especially pertinent under the new Eurodac and Interoperability Regulations. It is also relevant when it comes to determining to what extent the right of access to data and information may be restricted with regard to security-related information.

From an access to justice perspective, the question is not only whether a right is justiciable in theory but also whether access to it is ensured and realised in practice.[1193] With regard to national case law, this study was not able to comprehensively cover national case law in the EU. Nevertheless, it will offer some insights. The information and cases gathered below provide an indication of how certain issues are dealt with at national level. In general, it must be emphasised that case law on Eurodac data-related

1190 'Italy: The end of the systematic denial of data protection rights?' (*Statewatch,* 04 March 2025) <https://www.statewatch.org/analyses/2025/italy-the-end-of-the-systematic-denial-of-data-protection-rights/>; Italy was even giving misleading information on whether or what data is stored in SIS II ('Italian police are "misleading" people about Schengen entry bans, says internal EU report' (*Statewatch,* 24 February 2025) <https://www.statewatch.org/news/2025/february/italian-police-are-misleading-people-about-schengen-entry-bans-says-internal-eu-report/>.

1191 *Ligue des droits humains* (n 876) para. 70.

1192 The EDPS has recently detected various issues regarding the implementation of access rights: EDPB '2024 Coordinated Enforcement Action Implementation of the right of access by controllers' (16 January 2025).

1193 See chapter: Access to Justice.

questions is scarce; and thus far, it only deals with cases that arose under the old Eurodac Regulation 603/2013 and its predecessors. There is also no interoperability case law as of yet.

a) *Access to Information on Law Enforcement Access*

This study sought to find out more about the access of national law enforcement authorities to Eurodac data. According to eu-LISA's latest annual report on Eurodac, there were 1,491 searches conducted by national law enforcement authorities in Category 4 in 2023. This represents a 234% increase from 2021, and a 244% increase compared to 2019. Of these searches in this category, 98% were carried out by Germany (1,396), followed by Austria (33), France (18), Denmark (10), and Sweden (10).[1194] As part of this study, a request was made to the German Federal Criminal Police Office (*Bundeskriminalamt, BKA*). The aim was to determine whether information is available on how many access requests were granted. Additionally, the study sought to find out which data accesses were actually utilised in criminal proceedings. It also inquired whether convictions were handed down in these cases. Finally, the request aimed to ascertain whether access to Eurodac data was sought based on the suspicion that the data subject was a victim, perpetrator, or witness to a criminal offence. No reply to this question has been received. A similar request which was made public was answered negatively, stating that the BKA does not have such information.[1195] Furthermore, a public request regarding audit reports by the BKA on the admissibility of requests by law enforcement authorities to Eurodac was denied, citing confidentiality obligations.[1196]
It should be added that the monitoring and evaluation obligation with re-

1194 eu-LISA, 'Eurodac 2022 Annual Report' (2023) 18.

1195 Anfrage #297222 vom BKA, 'Ihr Antrag nach dem Informationsfreiheitsgesetz [IEG] hier: Jahresberichte über Wirksamkeit des Abgleichs von Fingerabdruckdaten mit Eurodac-Daten für Gefahrenabwehr- und Strafverfolgungszwecke' (1 February 2024) (*FragDenStaat*, 2024) <https://fragdenstaat.de/anfrage/jahresbericht-ueber-den-zugang-der-gefahrenabwehr-und-strafverfolgungsbehoerden-zu-eurodac/>.

1196 Anfrage #280747 von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 'Ihr Antrag nach dem Informationsfreiheitsgesetz - Prüfberichte EURODAC' (27 June 2023) (*FragDenStaat*, 2024) <https://fragdenstaat.de/anfrage/jahresbericht-ueber-den-zugang-der-gefahrenabwehr-und-strafverfolgungsbehoerden-zu-eurodac/>.

gard to access to Eurodac data by law enforcement authorities has not (yet) been fulfilled at European level. In a request to the European Commission to publish all annual reports on access to Eurodac by law enforcement authorities drawn up since 2015 in accordance with Art. 40(8) Eurodac Regulation 603/2013, the Commission stated that the requested annual reports were not available. The Commission indicated that it has not produced them, contrary to its legal obligation under Art. 40(8) Eurodac Regulation 603/2013.[1197]

b) *Access to Eurodac Data in Migration Procedures*

In two cases from 2007 in the United Kingdom (UK), the courts addressed the qualification of a Eurodac hit in terms of evidence. At that time, the UK was still part of the EU, and the Eurodac Regulation was applicable. The key issues were determining how a Eurodac hit should be classified and which standard of proof should be applied. These questions are dealt with in the chapter on the right to an effective remedy. However, a passage in one of these cases, YI, dealing with the question of access to Eurodac data shall be pointed out here. The Court held that an "Immigration Judge, acting fairly, would need to be satisfied on the specific evidence in each case whether that Appellant had indeed made a previous [asylum] claim. […] An Immigration Judge will also, as a matter of fairness, have to be satisfied that the Appellant has had the facility to access information about the assertion against him that would enable him, if he so wishes, to make a meaningful forensic rebuttal beyond mere denial. Of course, an Appellant may not want to use such a facility if the match is genuine and further evidence would only make matters worse for him. It is therefore the availability of the facility rather than the take-up that is needed in a fair system."[1198] This is an important point. Access to data is a prerequisite for a person to be able to question and challenge a Eurodac hit or a security flag, for example. As the English judge aptly points out, this opportunity must be provided to ensure a fair procedure. For this, not only access to Eurodac

1197 'Jahresbericht über den Zugang der Gefahrenabwehr- und Strafverfolgungsbehörden zu Eurodac - Anfrage an: Europäische Kommission' (*FragDenStaat*, 2024) <https://fragdenstaat.de/anfrage/jahresbericht-ueber-den-zugang-der-gefahrenabwehr-und-strafverfolgungsbehoerden-zu-eurodac/>.

1198 YI (Previous Claims - Fingerprint Match - EURODAC) *Eritrea v Secretary of State of Home Department* [2007] UKAIT 0054.

data must be provided in a way that the data subject can make a meaningful forensic rebuttal. This means that the bare information, that there was, e.g., a fingerprint match with a data set in another Member State, will not be enough. More information must be provided on how a hit was generated and what measures were taken to confirm it.

Access to information requests have, in some national cases, been restricted, based on security-related considerations. With regard to Eurodac data, no such case could be found. This might likely change once the security flags have been introduced in practice. However, related cases exist. For example, in Slovenia, an applicant's request to have his subsidiary protection extended was rejected. The Administrative Court concerned confirmed the negative decision, based on classified information to which the applicant did not have access. It considered the proceedings lawful, although the applicant was not given the possibility to be heard. Upon request for a revision of the decision, the Supreme Court (*Vrhovno sodišče*) held that it is important to clarify through jurisprudence whether, in such cases, national legislation is compliant with the recast Asylum Procedures Directive. Further, it is important to clarify whether the applicant, who does not have access to classified information, should have had access to legal aid and procedural safeguards to ensure his right to defence. The Supreme Court granted leave to revise the decision.[1199] These considerations must certainly be applied in connection with access to Eurodac data (especially regarding security flags), in accordance with the Eurodac or Interoperability Regulation. Corresponding procedural guarantees should be guaranteed at national level.

c) *Access to Eurodac by Authorities*

In Germany, two interesting cases have emerged that do not deal with the data subject's right of access. These cases concern the question as to which or whether any authority in Germany has been authorised to access Eurodac. First, the Administrative Court Wiesbaden (*Verwaltungsgericht*) found that Germany has not authorised any authority to access the Eurodac system, with the consequence that all access to the Eurodac system is unlaw-

1199 VS00050319 (Vrhovno sodišče, Upravni oddelek (Supreme Court, Administrative Department), 13.10.2021, ECLI:SI:VSRS:2021:X.DOR.198.2021.3, Slovenia).

ful.[1200] It investigated whether the BKA or the BAMF were authorised. In its analysis, the Court concluded that there was no legally valid designation within the meaning of Art. 27(2) Eurodac Regulation 603/2013 for either of them to access the Eurodac central system. A national authorisation provision was also missing. Accordingly, all access to the Eurodac system was unlawful, due to the lack of a designation of a competent authority.[1201] Just a few months later, the Administrative Court of Cologne (*Verwaltungsgericht*) decided otherwise.[1202] The Court stated that there was no difference between the old Eurodac Regulation 603/2013 and the revised version concerning which Member State was responsible for data collection, transmission, and processing of asylum applications. Therefore, national law designating the authority responsible for access to Eurodac did not need to be amended. The Court stated that it can be clearly determined who is responsible for what at national level (the BAMF or BKA). Nationally, the internal relationship between the BAMF and the BKA is regulated by Art. 16 Asylum Act: the BKA provides administrative assistance. Under European law, the BAMF alone is competent and responsible in accordance with Art. 27(2) Eurodac Regulation 603/2013.

These cases show how important it is to be able to check whether access to Eurodac data by the authorities was lawful – because this will not always be the case. As shown above, the data subject is only given this possibility to a very limited extent. It would be all the more important, now that the right of access to Eurodac data has been extended in this way.

4. Conclusions

The analysis of the Eurodac and Interoperability Regulations, alongside relevant case law, reveals both a clear right and persistent challenges in ensuring full access to personal data across EU Member States. The Eurodac and Interoperability Regulations both establish a right for data subjects to access their personal data and information. Access rights are crucial for transparency, accountability, and safeguarding individual rights, particularly in sensitive contexts such as asylum and law enforcement.

Despite this seemingly regulatory clarity, practical and implementation challenges persist. Data subjects may need to submit parallel requests under

1200 Verwaltungsgericht Wiesbaden, 21. September 2017, 6 L 3805/17WIA.
1201 ibid.
1202 Verwaltungsgericht Köln, 7. Dezember 2017, 5 L 4378/17A.

the Eurodac Regulation, the Interoperability Regulation, and the GDPR, depending on the information sought and their location. They may have to travel and provide biometric data to obtain access to Eurodac data. Procedures also vary depending on the Member State in which the request is lodged: some provide user-friendly model forms, while others require self-drafted requests, sometimes asking for reasons and for precise specification of the data sought. No EU-wide mechanism exists to manage requests for access, rectification, and erasure.

Furthermore, the scope of the right of access for data subjects remains unclear. There are indications that, in practice, it will not be sufficiently broad to ensure full access to information and thus effective access to justice. This is particularly evident with respect to crucial issues such as the extent of accessible data relating to hits or the security flag. The introduction of security-related measures, including security flags, poses significant challenges in balancing access rights with security imperatives. In this regard, it should be emphasised that only narrowly tailored exceptions to the right of access are allowed, in order to ensure compliance with fundamental rights standards. It should also be recalled that Eurodac is, at its core, a migration law instrument rather than a surveillance tool.

It has also become apparent that Eurodac and the Interoperability Regulations offer only limited transparency regarding who has accessed Eurodac data and how these data have consequently been used. Questions persist concerning the availability of information about data recipients, transfers to third countries, international organisations and private actors, as well as detailed records and logs of processing operations. Even with respect to automated decision-making within the MID, the Interoperability Regulations do not guarantee that data subjects can access meaningful information on the technologies employed or the underlying logic.

Moreover, although case law recognises the justiciability of the right of access, existing figures on access requests reveal substantial enforcement deficits. Moreover, detailed information on law-enforcement access to Eurodac is lacking, and the monitoring and evaluation obligations regarding such access have not been fulfilled at the European level. Taken together, these shortcomings underscore the need for more robust procedural safeguards to ensure that the right of access is effective in practice rather than merely formal.

To strengthen access to justice and improve the practical exercise of access rights, several measures should be considered. These include harmonising procedural standards across Member States, enhancing transparency

by allowing access to documentation on hits and core information about flags, key processing operations, and data recipients, and clarifying the legal scope of access rights and their exceptions. A broad and effective interpretation of the right of access should be promoted, provided this does not compromise legitimate security interests or ongoing investigations. Given that data subjects outside the Schengen Area often face significant hurdles in providing biometric or other identifying data, an effective mechanism should be established to ensure they can exercise their access rights in practice. The development of a unified, user-friendly portal for submitting requests would be beneficial.

Addressing the current gaps requires coordinated regulatory and practical efforts to ensure meaningful implementation, protect fundamental rights, and foster trust in EU data-processing systems. Much of the necessary progress will likely depend on litigation – a demanding route for many asylum seekers, for whom data protection is not a primary concern and who may lack access to specialised legal support. Clear guidance and sensitive implementation measures are therefore essential. Given the system's built-in potential for expanding processing operations and recipients, continued vigilance and adaptation to evolving legal and technological landscapes remain crucial to safeguarding individual rights.

III. The Right to Rectification, Completion, Erasure and Restriction of Processing of Personal Data and Information

1. What Is the Right to Rectification, Completion, Erasure, and Restriction of Processing?

The right to rectification and completion of personal data gives the data subject a subjective right against the controller to request them to rectify inaccurate and incomplete data stored about them. The provision thus supplements the objective principle of data accuracy stipulated in Art. 5(1)(d) GDPR.[1203] The secondary law provisions of Art. 43 Eurodac Regulation and Art. 48 Interoperability Regulations substantiate the primary law's right to rectification in Art. 8(2) sentence 2 CFR, stating that "[e]veryone has the right to obtain access to data which has been collected concerning him or her and to have it rectified".[1204]

Similarly, the right to erasure and restriction of processing of personal data gives data subjects a subjective right against the controller to request the erasure or restriction of processing of unlawfully stored data about them, when data are not (any longer) required or are inaccurate.[1205] The

1203 cf Cécile de Terwangne, 'Article 16 - Right to Rectification' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 473; cf also Tobias Herbst, 'Artikel 16 - Recht auf Berichtigung' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020), para 2; Lukas Feiler, Nikolaus Forgo, Michaela Weigl *The EU General Data Protection Regulation (GDPR): A Commentary* (2nd edn, Globe Law and Business Ltd 2018) 118.

1204 de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 473; Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 3.

1205 Herke Kranenborg, 'Article 17 - Right to Erasure ("Right to Be Forgotten")' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 479; Alexander Dix, 'Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden")' in Spiros Simitis, Gerrit Hornung and Indra Spiecker (eds), *Datenschutzrecht - DSGVO mit BDSG* (1st edn, Nomos 2019), para 1; Tobias Herbst, 'Artikel 17 - Recht Auf Löschung ("Recht Auf Vergessenwerden")' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020) para 17 f.; cf also Feiler, Forgo, Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* (n 1203) 120.

right forms part of the principles of data minimisation, data accuracy, and storage limitation, as stated in Art. 5(1)(c), (d) and (e) GDPR.[1206]

These rights are an expression of privacy rights in human rights instruments, as will be shown below. They are part of the basic principles of European data protection law and the corresponding case law. This chapter examines what these rights mean in the context of Eurodac data. It explores whether and how they can be exercised from an access to justice perspective.

a) *International Human Rights Law Applicable in Europe*

International human rights instruments generally enshrine the right to rectification, completion, erasure and restriction of processing of personal data as part of the right to privacy. While the UDHR is not binding, it still provides a right to privacy in Art. 12. Art. 17 ICCPR provides a binding right to privacy, which includes the right to rectify and erase personal data. Regarding Art. 17 ICCPR, the UN's Human Rights Committee (HRC) has stated that: "If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[1207] In Van Hulst v The Netherlands, the HRC stated that the right to privacy implies that every individual should have the right to request rectification or elimination of incorrect personal data in files controlled by public authorities.[1208] Under the UN's human rights frameworks, Art. 16 CRC and Art. 22 CRPD also provide a right to privacy, which includes the right to rectify and erase personal data.[1209]

1206 Dix, 'Artikel 17 - Recht Auf Löschung ("Recht Auf Vergessenwerden")' (n 1205), para 1; Herbst, 'Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden")' (n 1205), para 21, also includes the principle of purpose limitation in GDPR, Art 5(1)(b).

1207 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (UN Human Rights Committee (HRC) 1988), s 10.

1208 'Communication No. 903/2000, *Van Hulst v The Netherlands* (Views adopted on 1 November 2004, eighty second session)' (2004) CCPR/C/82/D/903/2000; 'Revised Views Adopted by the Committee under Article 5(4) of the Optional Protocol, Concerning Communication No. 2326/2013' (UN Human Rights Committee (HRC) 2018) CCPR/C/120/D/2326/2013/Rev. 1.

1209 cf UN Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' (UN Convention on

Art. 8 ECHR does not contain any data protection-specific provisions. However, it has been developed by the ECtHR into a fundamental right to data protection.[1210] The ECtHR examined several cases concerning the storage by authorities of false data or data whose accuracy was disputed by the applicant under the right to respect for private and family life in Art. 8 ECHR,[1211] and emphasised that the inability to rectify personal data is an interference with their right to respect for private life.[1212] However, the Court has held that limitations on the ability to rectify personal data can be justified, particularly in circumstances involving state security, national defence, or public security.[1213] The ECtHR held that there is a positive obligation for a State Party to the ECHR to allow natural persons to provide objective evidence in view of having personal data relating to them changed (*in casu* their official ethnicity).[1214] The Court has addressed the issue of the right to deletion of personal data under Art. 8 ECHR.[1215] It has emphasised the need for effective safeguards to ensure the deletion of personal data

---

the Rights of the Child 2021) CRC/C/GC/25 25; Mario Viola de Azevedo Cunha, 'Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy' [2017] UNICEF, Innocenti Discussion Paper; Mark C Weber, 'Protection for Privacy under the United Nations Convention on the Rights of Persons with Disabilities' (2017) 6 Laws, no 3; cf also United Nations Development Program (UNDP), 'Drafting Data Protection Legislation: A Study of Regional Frameworks' (2023).

1210 Paul Peuker, 'Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden")' in Gernot Sydow and Nikolaus Marsch (eds), *Datenschutz-Grundverordnung | Bundesdatenschutzgesetz* (3rd edn, Nomos 2022), para 7.

1211 cf *Torsten Leander v Sweden* (n 523), para 48; *Rotaru v Romania* (n 865), para 46; *Ciubotaru v Moldova* App no 27138/04 (ECtHR, 27 April 2010), paras 58 - 59; *Cemalettin Canlı v Turkey* App no 22427/04 (ECtHR, 28 Nov 2008), para 41ff; *Khelili v Switzerland* App no 16188/07 (ECtHR, 18 Oct 2011).

1212 *Ciubotaru v Moldova* (n 1211), para 59; *Torsten Leander v. Sweden* (n 523), para 48; *Rotaru v. Romania* (n 865), para 46.

1213 cf *Gheorghe Dalea v France* (n 1079).

1214 *Ciubotaru v Moldova* (n 1211), paras 58 - 59.

1215 cf *M.L. and W.W. v Germany* App nos 60798/10 and 65599/10 (ECtHR, 28 June 2018); *B.B. v France* [1998] ECHR 1998-VI; *Gardel v France* App no 16428/05 (ECtHR, 17 Dec 2009); *M.B. v France* App no 22155/06 (ECtHR, 17 Dec 2009); *M.K. v France* App no 19522/09 (ECtHR, 18 April 2013); *Brunet v France* [2014] ECHR 263; *Aycaguer v France* App no 8806/12 (ECtHR, 22 June 2017); *Catt v the United Kingdom* App no 43514/15 (ECtHR, 24 April 2019); *Gaughran v the United Kingdom* App no 45245/15 (ECtHR, 13 Feb 2020); *M.M. v the United Kingdom* App no 24029/07 (ECtHR, 13 Nov 2012); *Segerstedt-Wiberg and Others v Sweden* (n 864).

when their continued retention becomes disproportionate.[1216] The ECtHR also discussed a 'right to be forgotten' in Węgrzynowski and Smolczewski v Poland but has not decided (yet) that this exists.

Finally, Art. 8(c) of Convention 108 and Art. 9(e) of the Modernised Convention 108+ state the right of the data subject "to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention". Exceptions and restrictions are stipulated in Art. 11 of the Modernised Convention 108+.

b) *EU Human Rights Law: The European Charter of Fundamental Rights*

The CFR provides, in Art. 7, the respect for private and family life. Art. 8 CFR delineates the protection of personal data, stating explicitly "the right to have [data which has been collected concerning him or her] rectified." Art. 8 CFR recognises the principle of accuracy, which requires the data to be accurate and, where necessary, kept up to date. All reasonable measures must be taken to ensure that inaccurate personal data, in relation to the purposes for which they are processed, are erased or corrected without delay.[1217] The CJEU has consistently emphasised the significance of the right to rectification. In its case Nowak, the ECJ considered a request for access under the DPD with a view inter alia to possible rectification.[1218] In its Opinion 1/15, the ECJ clarified that notification of who accessed a person's data is essential. This allows the individual to be confident that their personal data are being processed correctly and lawfully. It also enables them to exercise their right of access and, if needed, the rectification of those data. Additionally, under Art. 47 CFR, it ensures the right to an effective remedy before a tribunal.[1219] In its case Schrems I, the Court made an explicit link between data protection rights, including the right to rectification and the fundamental right to effective legal protection enshrined in

1216 *Catt v the United Kingdom* (n 1215), para 119; *Gaughran v the United Kingdom* (n 1215), para 94.

1217 Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 08.138.

1218 *Peter Nowak v Data Protection Commissioner* (n 1033), para 49.

1219 Opinion 1/15 on the Draft Canada-EU PNR Agreement (n 541), para 219ff; cf also Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 08.162.

Art. 47 CFR.[1220] According to the Court, the essence of the fundamental right to effective judicial protection is not respected if an individual does not have the possibility to "pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data".[1221] The right to erasure was also considered by the CJEU in the Manni case, which dealt with a request to remove certain personal data from a public companies register.[1222] It held that only in "specific situations, overriding and legitimate reasons relating to the specific case of the person concerned could justify, exceptionally, that access to personal data concerning him should be limited".[1223] However, the ECJ incorporated in Art. 8 CFR, according to some scholars, a right to be forgotten in its judgment Google Spain SL.[1224] Others argue that this was not the case.[1225] Nevertheless, this right to be forgotten is now explicitly contained in Art. 17 GDPR.

When interpreting the above-mentioned provisions, the CJEU regularly takes into account[1226] the case law of the ECtHR on the right to respect for private and family life in Art. 8 ECHR.[1227]

1220 *Schrems v Data Protection Commissioner* (n 175); de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 473.

1221 *Schrems v Data Protection Commissioner* (n 175), para 95.

1222 Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* [2017] OJ C 144/6.

1223 ibid, para 60.

1224 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] OJ C 212/4; Kranenborg, 'Article 8 – Protection of Personal Data' (n 537), para 08.172; Lock, 'Article 8 CFR' (n 540), para 16.

1225 Peuker, 'Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden")' (n 1210), para 7, stating that the CFR does not recognise an independent "internet fundamental right to be forgotten" - such a right has not been developed by the CJEU in the further development of judicial law from existing fundamental rights.

1226 cf Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* [2003] ECR I-4989, para 67ff; Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECR I-2971, para 87.

1227 Peuker, 'Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden")' (n 1210), para 7, referencing *Torsten Leander v Sweden* (n 523), para 48; *Amann v Switzerland* [2000] ECHR 2000-II, para 65; *Rotaru v Romania* (n 865), para 43; *Segerstedt-Wiberg and Others v Sweden* (n 864), para 72; *S and Marper v United Kingdom* (n 732), para 103.

c) *EU Law: GDPR, Police Directive and Data Protection Directive for EU Institutions and Bodies*

aa) General Data Protection Regulation

The GDPR has a broad scope, as has been discussed in the last chapter,[1228] and is, according to Art. 3, applicable to data processed in the Eurodac and Interoperability systems, even if the data subject concerned resides outside of the Schengen Area.

Art. 16 GDPR contains the right to rectification and completion, stating that the data subject has a right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. The data subject further has the right to have incomplete personal data completed, including by means of providing a supplementary statement, when it seems necessary with regard to the purpose of the processing.[1229]

The right to erasure is stipulated in Art. 17 GDPR. The data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay. The controller bears the obligation to erase personal data where one of six reasons applies: the personal data are no longer necessary for the purposes for which they were collected or processed; the data subject withdraws their consent in cases where processing is based on it or objects to the processing; personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation; or the personal data have been collected in relation to the offer of information society services. Specific rules apply to information that has been made public.[1230] There are several reasons based on which the keeping of data can be justified. This is the case when processing is necessary for exercising the right of freedom of expression and information; for compliance with a legal obligation which requires processing by Union or Member State law; or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical

1228 See chapter: The Right to Access Personal Data and Information.

1229 cf de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 473; Alexander Dix, 'Artikel 16 - Recht auf Berichtigung' in Spiros Simitis, Gerrit Hornung and Indra Spiecker (eds), *Datenschutzrecht - DSGVO mit BDSG* (1st edn, Nomos 2019), para 6 and 18ff; Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 28ff.

1230 GDPR, Art 17(2).

research purposes or statistical purposes, or for the establishment, exercise, or defence of legal claims.[1231]

The GDPR includes a specific right to the restriction of processing under Art. 18. A data subject can request restriction of processing in four situations. First, when the accuracy of personal data is contested by the data subject, allowing time for the controller to verify its accuracy. Second, if the processing is unlawful but the data subject opposes erasure and instead requests restricted use. Third, when the controller no longer needs the data for processing, but the data are required by the data subject for legal claims. Lastly, if the data subject has objected to processing under Art. 21(1) GDPR, pending verification of whether the controller's legitimate grounds override those of the data subject. In the context of Eurodac, the first reason seems particularly likely to occur. When processing has been restricted, the personal data can only be processed under certain conditions. Aside from storage, processing is allowed with the data subject's consent. It may also be processed for the establishment, exercise, or defence of legal claims. Additionally, processing is permitted to protect the rights of another natural or legal person. Finally, it can be processed for reasons of important public interest of the Union or a Member State.[1232] A data subject who has obtained restriction of processing must be informed by the controller before the restriction of processing is lifted.[1233]

Finally, Art. 19 GDPR contains a notification obligation regarding rectification, erasure, or restriction of processing of personal data. The controller has to communicate any rectification, erasure, or restriction of processing carried out in accordance with Art. 16, 17(1) and 18 GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller has to inform the data subject about those recipients if the data subject requests it.

Regarding the exercise of these rights, the general provision in Art. 12 GDPR is applicable. This article stipulates that the controller must provide information to the data subject in a concise, transparent, intelligible, and easily accessible form.[1234] Additionally, after a request is made, the controller is required to inform the data subject of the actions taken in response to their request.[1235] Actions taken are free of charge, unless re-

1231 ibid, Art 17(3).
1232 ibid, Art 18(2).
1233 ibid, Art 18(3).
1234 ibid, Art 12(1).
1235 ibid, Art 12(3).

quests from a data subject are manifestly unfounded or excessive.[1236] Also, Art. 12(4) GDPR holds that if the controller does not take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of the reasons for not taking action and on the possibility of lodging a complaint. Whenever the controller has reasonable doubts concerning the identity of the natural person making a request, it may request additional information necessary to confirm the identity of the data subject.[1237]

According to Art. 16 GDPR, the data controller must rectify data without undue delay. In no case may the rectification period exceed the one-month period of Art. 12(3) GDPR.[1238] Both Union law and Member State law may provide for exceptions to the right of rectification where such rectification would, for example, prejudice the achievement of scientific research or statistical purposes.[1239]

Finally, the general limitations in Art. 23 GDPR apply to the rights mentioned in this section. They are based mainly on security concerns, the prevention or investigation of criminal offences and other important objectives of general public interest of the Union or of a Member State.

1236 ibid, Art 12(5).

1237 ibid, Art 12(7).

1238 According to Alexander Dix, 'Artikel 18 - Recht auf Einschränkung der Verarbeitung' in Spiros Simitis, Gerrit Hornung and Indra Spiecker (eds), *Datenschutzrecht - DSGVO mit BDSG* (1st edn, Nomos 2019), para 4, and Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), no 17, there is no possibility of an extension: "Since Art. 16 does not refer to this more flexible provision [in GDPR, Art 12], but is content with the adjective "without delay", there is no possibility of extension in the case of rectification, just as there is in the case of deletion (Art 17, para. 4); this opinion is not shared by other authors, such as: Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 24 and Paul Peuker, 'Artikel 16 - Recht auf Berichtigung' in Gernot Sydow and Nikolaus Marsch (eds), *Datenschutz-Grundverordnung | Bundesdatenschutzgesetz* (3rd edn, Nomos 2022), para 13.

1239 GDPR, Art 89(2) and (3); furthermore, according to ibid, Art 85(2), Member States may provide for derogations and exemptions from the right of rectification in the case of processing for journalistic, scientific, artistic or literary purposes where this is necessary to reconcile the right to data protection with the right to freedom of expression and information; cf Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 19.

bb) Data Protection Regulation for EU Institutions and Bodies

Art. 18, 19 and 20 of the Data Protection Regulation for EU institutions and bodies provide for the right to rectification and erasure of personal data and restriction of processing thereof, which largely overlaps with these rights in the GDPR. Furthermore, there is, in Art. 21 Data Protection Regulation, a notification obligation regarding rectification or erasure of personal data or restriction of processing. Restrictions to this right apply according to Art. 25 Data Protection Regulation for EU Institutions and Bodies. They are based mainly on security concerns, the prevention or investigation of criminal offences, and other important objectives of general public interest of the Union or of a Member State.

cc) Police Directive

The Police Directive also contains a similar right to rectification or erasure of personal data and restriction of processing in Art. 16. The article states that Member States must ensure the controller informs the data subject in writing of any refusal to rectify or erase personal data or restrict processing. The controller must also provide the reasons for the refusal. However, Member States may adopt legislative measures to restrict this obligation, either wholly or partly. Such restrictions must be necessary and proportionate in a democratic society. They must also consider the fundamental rights and legitimate interests of the concerned individual. Restrictions can be imposed to protect public or national security, the freedoms of others, or to avoid obstructing official or legal inquiries, investigations, or procedures. They may also be necessary to prevent, detect, investigate, or prosecute criminal offences, or to carry out criminal penalties.

d) *Eurodac Regulation and AMMR*

The Eurodac Regulation contains a right to access, rectification, completion, erasure, and restriction of the processing of personal data in Art. 43. The rights have to be exercised in accordance with Chapter III of the GDPR (Art. 12 ff.) and applied as set out in the Eurodac Regulation.[1240]

1240 Eurodac Regulation 2024, Art 43(1).

If the rights of rectification and erasure are exercised in a Member State other than the one that transmitted the data, the authorities of that Member State must contact the authorities of the transmitting Member State. This is necessary so that the latter can verify the accuracy of the data. Additionally, they must check the lawfulness of both the data's transmission and their recording in Eurodac.[1241]

If data recorded in Eurodac are factually inaccurate or have been recorded unlawfully, the Member State that transmitted them has to rectify or erase them in accordance with Art. 40(3) Eurodac Regulation. That Member State has to confirm in writing to the data subject that it has taken action to rectify, complete, erase, or restrict the processing of personal data relating to them. [1242]

If, however, the Member State that transmitted the data does not agree that data recorded in Eurodac are factually inaccurate or have been recorded unlawfully, it has to explain in writing to the data subject why it is not prepared to correct or erase the data.[1243]

That Member State must provide the data subject with information explaining the steps which they can take if they do not accept the explanation provided. This must include information on how to file an action or, if applicable, a complaint before the competent authorities or courts of that Member State. It should also provide details on any financial or other assistance available in accordance with the laws, regulations, and procedures of that Member State.[1244]

The competent authorities of the Member States must cooperate actively to enforce promptly the data subject's rights to access, rectification, completion, erasure, and restriction of processing. [1245] There are no deadlines within which the Member States have to act.[1246]

Any request for access, rectification, completion, erasure, and restriction of processing has to contain "all the necessary particulars to identify the data subject, including biometric data".[1247] Such data should be used exclusively to permit the exercise of the data subject's rights; they have to

1241 ibid, Art 43(2).
1242 ibid, Art 43(4).
1243 ibid, Art 43(5).
1244 Ibid.
1245 ibid, Art 43(7).
1246 Other than in GDPR, Art 12(4).
1247 Eurodac Regulation 2024, Art 43(6).

be erased immediately afterwards.[1248] Unlike access requests, the Eurodac Regulation does not stipulate that a written record must be created and made available to the supervisory authority for requests related to rectification, completion, erasure, or restriction of processing.[1249]

The national supervisory authority of the Member State that transmitted the data, as well as the national supervisory authority of the Member State where the data subject is present, must provide information to the data subject upon request. This information concerns the exercise of their right to request access, rectification, completion, erasure, or restriction of the processing of their personal data from the data controller. The supervisory authorities cooperate in accordance with Chapter VII of the GDPR.[1250]

According to Art. 60 Eurodac Regulation, its provisions are not applicable to any territory to which the AMMR does not apply.[1251] This means that for data subjects outside the Schengen Area, these provisions seem not to apply. Since their data are still processed by a processor in an EU Member State, the GDPR applies.[1252]

e) *Interoperability Regulation*

The Interoperability Regulation, according to Art. 3, applies to individuals whose personal data may be processed in the EU information systems. This includes Europol data, which can be queried simultaneously with the EU information systems mentioned. Consequently, it applies to data subjects, regardless of whether they reside inside or outside the Schengen Area.

The Interoperability Regulation holds in Art. 48 the right to (access), rectification, erasure, and restriction of personal data stored in the MID. There is no provision stipulating these same rights with regard to data stored in the CIR or the sBMS.

The Interoperability Regulation refers in Art. 48 to the rights in Art. 15 to 18 GDPR, Art. 17 to 20 Data Protection Regulation of Union Bodies and Art. 14, 15 and 16 Police Directive, only providing few additional procedural requirements with regard to these rights. Even though the right to comple-

1248 ibid, Art 43(6).
1249 ibid, Art 43(8).
1250 ibid, Art 43(9).
1251 The AMMR applies to Member States (and Schengen/Dublin-Associated States). According to ibid, Art 76, [a]s far as the French Republic is concerned, this Regulation shall apply only to its European territory.
1252 GDPR, Art 3.

tion of data is not mentioned explicitly in the Interoperability Regulations, it still exists, since the right to rectification in Art. 15 GDPR, to which the Interoperability Regulations refer, includes the right to completion of data.

Data subjects can address themselves to the competent authority of a Member State, in order for them to rectify, erase, or restrict the processing of their personal data.[1253] The Interoperability Regulations state in Art. 48(2) a specific period of 45 days, with a possible extension of another 15 days, in which a request must be examined. The Member State has to inform the data subject of such an extension within the 45-day period.[1254]

If a request for rectification or erasure of personal data is made to a Member State other than the one responsible for manual verification of different identities, the following procedure applies. The Member State receiving the request must contact the authorities of the responsible Member State. This applies to cases where the ETIAS Central Unit was involved as well. This communication must occur within seven days. They, in turn, have to respond within 30 days, with a possible extension of another 15 days.[1255] These provisions, stating time limits, do not mention access and restriction requests.

Where data stored in the MID are inaccurate or have been recorded unlawfully, the responsible Member State has to rectify or erase those data. The person concerned must be informed in writing about this.[1256] If a Member State is not prepared to rectify or erase data, it has to adopt a written administrative decision.[1257] Here, too, requests for access and restriction are not mentioned in the law.

Art. 48(8) Interoperability Regulation states that if a Member State issues a negative decision, it must provide the individual with information about their rights. This includes an explanation of how to challenge the decision regarding requests for access, rectification, erasure, or restriction of processing of personal data. Additionally, the Member State must inform the person about how to bring an action or complaint before the competent authorities or courts. Relevant assistance, including support from supervisory authorities, should also be included.

1253 Interoperability Regulation - Judicial Cooperation, Art 48(1); Interoperability Regulation - Borders, Art 48(1).
1254 ibid, Art 48(2).
1255 ibid, Art 48(3) and (4).
1256 ibid, Art 48(5).
1257 ibid, Art 48(7).

Any requests have to contain the information necessary to identify the data subject. That information must be used exclusively to enable the exercise of the data subject's rights. It has to be erased immediately afterwards.[1258] Member States responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made have to keep written records of any request and make it available to the supervisory authorities without delay.[1259]

According to Art. 48(11) Interoperability Regulations, limitations and restrictions to the rights of rectification, erasure, and restriction pursuant to the GDPR and the Police Directive apply.

2. Scope and Limitations

a) *Who Can Request Rectification, Completion, Erasure and Restriction of Data?*

The rights to request rectification, completion, erasure, and restriction of processing of data in Art. 43 Eurodac Regulation and Art. 48 Interoperability Regulation are individual rights. They are addressed to data subjects whose personal data are recorded in Eurodac or the MID. There is a range of obstacles to accessing these rights, in particular for certain categories of data subjects, such as children and persons with disabilities, or persons living outside the Schengen Area. These obstacles have been addressed in detail in the chapter on the right to access personal data and information.[1260] Reference can be made to what was discussed there, since the same issues apply with regard to the rights discussed in this chapter.

b) *Which Data Can Be Rectified, Completed, Erased or Restricted for Processing?*

aa) Eurodac Regulation

Under the new Eurodac Regulation, much more biographic and new biometric data are stored in Eurodac and since it will be made interoperable,

1258 ibid, Art 48(9).
1259 ibid, Art 48(10).
1260 Chapter: The Right to Information.

even more data, such as biometric templates or links between data sets, are created. This section looks at which data can be rectified, completed, erased, or restricted for processing under the Eurodac Regulation.

aaa) *Personal Data and Information*

The Eurodac Regulation does not express explicitly which data can be rectified, completed, erased, or restricted for processing. However, the right to rectification is intrinsically linked to the right of access; once data subjects have accessed their personal information and discovered that it is inaccurate or incomplete with regard to the purpose of the processing, they have the correlated right to have the data rectified or completed.[1261] Accordingly, accessible information must also be subject to erasure and restriction of processing requests.[1262] Generally, the same data which can be accessed can be rectified, completed, erased, and restricted for processing.
In the last chapter on the right to access personal data and information, it was concluded that although the Eurodac Regulation provides in Art. 43 a right to access personal data, certain information that is not considered personal data can also be accessed.[1263] As the rectification and erasure rights are closely linked to the access right, they also concern personal data and, although seldom, information.[1264]

1261 de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 471.

1262 The right to erasure was also contained in the Data Protection Directive 95/46/EC in the provision on the right of access, Art 12; cf also GDPR, Recital 65; Eurodac Regulation 2024, Recital 82.

1263 Chapter: The Right to Information.

1264 de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 473 talks about "erroneous or false information." In most cases however, information is only false, if erroneous personal data has been stored. For example, the information regarding the storage period might be false, but this normally will only occur, if the data subject is stored under a false category; for example, as an asylum seeker instead of an irregularly staying third-country national. False information might be stored, however, in a case where a hit is triggered with a data set in another database, but the hit turns out to be false. Then, such a hit is not 'personal data' but only false information.

bbb) *Eurodac Hit*

A Eurodac hit, indicating that personal data of a person are already stored in Eurodac, constitutes personal data in the sense of Art. 4(1) GDPR.[1265] This, as was argued in the last chapter, can be accessed under the right to access personal data and information. A Eurodac hit can also be rectified, or better, erased, if it turns out to be a false hit.

Under the new Eurodac Regulation, and different from Eurodac Regulation 603/2013,[1266] the results of fingerprint comparison are not always checked by a fingerprint expert, but only "where necessary".[1267] So far, if the verification process under Art. 25 Eurodac Regulation 603/2013 was unable to confirm a hit, the Member State was required to report the false hit to eu-LISA and to the European Commission.[1268] In 2022, 111 false hits were reported by the Member States.[1269] This number has steadily increased over the last years.[1270] Whether this reflects the total number of false hits cannot be determined, as there is no assurance that Member States report all of them. As noted, a verification process only takes place "where necessary." When exactly a Member State must consider such verification necessary remains unclear and likely differs from one state to another. According to the French National Implementation Plan, "[t]he validation process is therefore to be largely automated"[1271], which only deepens the fog around when human oversight actually occurs. The Plan continues that "[t]he assignment of hits (currently comprising 80% of officials' tasks) is to be reduced to a limited volume. The updating of data in the Eurodac database (currently

1265 Art. 29 WP, 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 13: "The so-called "hit-flag" indicating that data on a person are stored in the CIR, constitutes personal data." A hit indicating that data is stored in Eurodac must, accordingly, also be considered personal data.

1266 Eurodac Regulation 603/2013, Art 25(4).

1267 Eurodac Regulation 2024, Art 38(4).

1268 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 23; for 2023, eu-LISA so far only provided the Eurodac 2023 Statistics, which does not contain numbers for false hits (eu-LISA, 'Eurodac 2023 Statistics - June 2024' (2024)).

1269 ibid 23.

1270 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 23.

1271 'PLAN NATIONAL DE MISE EN OEUVRE DU PACTE EUROPEEN SUR LA MIGRATION ET L'ASILE' (*Direction générale des étrangers en France,* Décembre 2024) 10 at 1.3.2.1: "Le processus de validation a donc vocation à être largement automatisé."

15% of tasks), which is already underway, should be fully automated by 2027."[1272] This study argues that, at a minimum, verification should occur where a data subject submits a substantiated claim that a hit is false. It is also conceivable that, in the future, fewer false hits will be reported simply because no fingerprint expert verifies the results. Statistically, this would appear as an improvement in Eurodac's technological accuracy, even though it may merely reflect a lack of verification.

Where a hit is produced for both fingerprints and facial images, Member States may check the result of the comparison of the facial image data. Only where a Eurodac hit is based solely on comparison of facial images, "an expert trained in accordance with national practice", shall immediately check and verify the result of the comparison.[1273] As we will see in the next chapter, the error rate for facial image matching is much higher than for fingerprint comparison.[1274] It therefore makes sense to consult an expert, at least in those cases.

In connection with access to Eurodac by law enforcement authorities, not only biometric data are compared; alphanumeric data can also be compared and produce a hit.[1275] In principle, such a hit must be contestable and, if applicable, its erasure requested. The problem here is that the data subject will probably not find out about such a hit when it occurs. They will likely only be informed about it later (during criminal investigation proceedings), if at all.[1276]

1272 ibid. 12 at 1.3.3: "L'adjudication des hits (80% des missions des agents actuellement) devrait être réduite à un volume limité. L'activité de mise à jour des données de la base Eurodac (15% des missions) aujourd'hui réaliséemanuellement devrait pouvoir être entièrement automatisée à partir de 2027."

1273 Eurodac Regulation 2024, Art 38(5). According to the 2016 Eurodac Proposal, Art 42(4), a feasibility study should have been done by 2020 to evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of Eurodac. The framework of the study, which will only evaluate the reliability and accuracy of the results produced from facial recognition software for the purpose of Eurodac, was furthermore criticised by the EDPP for lacking an analysis of the necessity and proportionality of the processing of facial images (D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298) 6). So far, the study has not been conducted.

1274 Chapter: The Right to an Effective Remedy.

1275 Eurodac Regulation 2024, Art 33(1) and 34(1).

1276 See chapters: The Right to Information, and The Right to Access Personal Data and Information.

ccc) *Security Flag*

Following the health, vulnerability, identity, and security checks as held in the Screening Regulation,[1277] Art. 16(4) AMMR and Art. 9(5) Asylum Procedure Regulation, the fact that a person could pose a threat to internal security is recorded in Eurodac if the person is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in the Terrorism Directive or in any of the offences referred to in the EAW Council Framework Decision."[1278] According to Art. 42(1)(c) Eurodac Regulation, the data subject concerned has to be informed about the fact that they are considered to be a threat to internal security and that the Member State of origin is obliged to register that fact in Eurodac. Data subjects should be able to refute the presumption of being a threat.[1279] For this, as seen in the last chapter, they need to be able to access the personal data and information that led to the conclusion of them being a security threat. They must be able to request rectification, completion, erasure, or restriction of processing of such data. However, these rights can be restricted in accordance with Art. 23 GDPR.[1280]

As discussed in the last chapter, the right to access certain data and information in the context of the security flag may in part be derived from the right to an effective remedy (and not the right to privacy). Similarly, the rights to rectification and completion of personal data can, to some extent, be derived from the right to an effective remedy and the right to good administration, particularly the right to be heard.[1281] The controller is obliged to verify contested data under the principle of accuracy and on

1277 Screening Regulation, Art 12 and 14 - 16.

1278 Eurodac Regulation 2024, Art 17(2)(i) and Recital 8. The list of offences covered by this directive is much shorter than was the case with earlier drafts of the new Eurodac Regulation. However, this limitation is offset by the potentially very broad and defined only in ibid, Recital 8, as "whether the person has displayed behaviour that results in physical harm to other persons that would amount to a criminal offence under national law".

1279 Evelien Brouwer, Giuseppe Campesi and Sergio Carrera, 'The European Commission's Legislative Proposals in the New Pact on Migration and Asylum' (EU Parliament, LIBE Committee) PE 679.130, 101.

1280 Eurodac Regulation 2024, Art 43(3).

1281 CFR, Art 41 and 47; cf Angela Ward, 'Article 47 - Right to an Effective Remedy and a Fair Trial' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Publishing 2021), para. 47.02; *Schrems v Data Protection Commissioner* (n 175), para 95.

the basis of the right of rectification.[1282] According to the right to be heard, the data subject must be able to argue that data stored in Eurodac are not accurate. Authorities and courts have to consider this and accept evidence to that regard, as will be shown in this section. However, as will be seen in the last section of this chapter, such claims are often not heard in practice.

Art. 47(2) CFR guarantees a right to a fair and public hearing by an independent and impartial tribunal and a possibility to be advised, defended, and represented. In addition, Art. 48 CFR guarantees the presumption of innocence and the right to defence and Art. 41 CFR the right to good administration. The right to a fair hearing constitutes a fundamental principle of EU law.[1283] It applies in all proceedings, including administrative proceedings.[1284] The obligation to provide a fair hearing is a core component of Art. 6 ECHR.[1285] It has been the subject of substantial litigation before both the ECtHR and the CJEU. The right to a fair hearing consists of

1282 Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 34; Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 17; Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), para 13.

1283 Case C-289/11 P *Legris Industries SA v European Commission* [2012] OJ C 174/13, para 36: "En tout état de cause, cette entrée en vigueur, comportant l'inclusion de la Charte dans le droit primaire de l'Union, ne saurait être considérée comme un élément de droit nouveau, au sens de la disposition susvisée du règlement de proc é dure de la Cour. En effet, il y a lieu de rappeler que, même avant l'entrée en vigueur de ce traité , la Cour avait d é j à constaté à plusieurs reprises que le droit à un procès équitable tel qu'il découle, notamment, de l'article 6 de la CEDH constitue un droit fondamental que l'Union européenne respecte en tant que principe général en vertu de l'article 6, paragraphe 2, UE (voir notamment Case C-305/05 *Ordre des barreaux francophones et germanophone and Others v Conseil des ministres* [2007] ECR I-5305, points 29 et 37)". (In any event, this entry into force, involving the inclusion of the Charter in the primary law of the Union, cannot be regarded as a new factor of law within the meaning of the aforementioned provision of the Court's Rules of Procedure. It should be borne in mind that, even before the entry into force of that Treaty, the Court had already found on a number of occasions that the right to a fair trial deriving, inter alia, from Article 6 of the ECHR is a fundamental right which the which the European Union respects as a general principle by virtue of by virtue of Article 6(2)).

1284 Case C-249/13 *Khaled Boudjlida v Préfet des Pyrénées-Atlantiques* [2014], para 31. It is affirmed in Charter of Fundamental Rights of the European Union [2000] OJ C364/1 (CFR), Art 47 and 48, which ensure respect for both the rights of the defence and the right to fair legal process, but also in ibid, Art 41, which guarantees the right to good administration.

1285 Sayers, 'Article 47 – Right to an Effective Remedy and to a Fair Trial' (n 1127), para 47.634.

several aspects, which are the principle of adversarial proceedings, equality of arms, and the right to a reasoned judgment.[1286]

In order to satisfy the requirements of the right to a fair hearing, it is important for the parties to be apprised of, and to be able to debate and be heard on, the matters of fact and of law which will determine the outcome of the proceedings.[1287] Parties should be able to participate effectively by knowing and understanding the case and by being able to comment on it and challenge it.[1288] The ECJ has reiterated in its case ZZ, which has already been discussed in the last chapter, that "having regard to the adversarial principle […], the parties to a case must have the right to examine all the documents or observations submitted to the court for the purpose of influencing its decision, and to comment on them."[1289] In Bensada Benallal, an EU citizen had made false statements to authorities which subsequently led to the withdrawal of his residence permit. However, the person concerned had not been heard before a decision on his residence permit was taken. This point was only raised on appeal. The ECJ decided that if this plea

1286 ibid, para 47.634ff.

1287 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559) para 47.97, with reference to Case C-543/14 *Ordre des barreaux francophones et germanophone and Others v Conseil des ministres* [2016] OJ C 350/4, para 41, and Case C-89/08 P *European Commission v Ireland, French Republic and Others* [2009] ECR I-11245, para 56.

1288 *Brandstetter v Austria* [1991] Series A no 211; *Ruiz-Mateos v Spain* [1993] 16 EHRR 505.

1289 *ZZ v Secretary of State for the Home Department*, (n 559) para 55. Cf also Case C-450/06 *Varec SA v Belgian State* [2008] ECR I-581, para 45 and *European Commission v Ireland, French Republic and Others* (n 1287), para 52. It also confirmed that any failure by the competent national authority to disclose to the person concerned, "precisely and in full, the grounds on which a decision […] is based and to disclose the related evidence to him is limited to that which is strictly necessary, and that he is informed, in any event, of the essence of those grounds in a manner which takes due account of the necessary confidentiality of the evidence *(ZZ v Secretary of State for the Home Department*, (n 559), para 69)." The CJEU also held that if, in exceptional cases, a national authority argued that full disclosure was not possible, it must have at its disposal and apply techniques and rules of procedural law which accommodate both legitimate security considerations and the need to ensure sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle (ibid, paras 56 - 57). In *Regner v Czech Republic* App no 35289/11 (ECtHR, 19 September 2019), the Grand Chamber of the ECtHR made reference to the CJEU's reasoning in *ZZ v Secretary of State for the Home Department* (n 559).

satisfies the conditions required by national law for it to be classified as a plea based on public policy, it is admissible before the appeal court.[1290]

In the area of asylum and immigration policy, there is a line of case law interpreting the right to an effective remedy in the context of the rights of asylum seekers challenging return or transfer under the Dublin III Regulation, as provided for under Art. 27(1) of that regulation,[1291] which is replaced by Art. 43 AMMR.[1292] In this field, there have been especially relevant developments linking the rights of the defence and the right to be heard.[1293] In the case of Boudjlida, the referring court asked the ECJ to clarify the scope of the right to be heard in all proceedings. Specifically, the court inquired whether this right includes the following for an illegally staying third-country national facing a return decision: 1) The right to access and analyse all information used against them that justifies the decision made by the competent national authority; 2) the right to an adequate period for reflection before submitting their observations; 3) the right to legal representation of their choice during the hearing.[1294] The Court reiterated earlier judgments, emphasising that the right to be heard guarantees every individual the opportunity to effectively express their views during an administrative procedure. This right is fundamental before any decision is made that could adversely affect their interests.[1295] This includes the right of third-country nationals to be heard before the adoption of a return decision concerning them.[1296] In accordance with the Court's case law, the ECJ stated that the purpose of the rule requiring the addressee of an adverse decision to be allowed to submit observations before that decision is adopted is to ensure that the competent authority can effectively consider all relevant information. To ensure that the person concerned is adequately

1290 Case C-161/15 *Abdelhafid Bensada Benallal v État belge* [2016] OJ C 156/18.

1291 And its scope as clarified in Dublin III Regulation, Recital 19, which nonetheless itself refers to CFR, Art 47.

1292 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.178.

1293 *Khaled Boudjlida v Préfet des Pyrénées-Atlantiques* (n 1284), paras 41 - 42; Case C-166/13 *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* [2014] OJ C 7/7, paras 51 - 52.

1294 *Khaled Boudjlida v Préfet des Pyrénées-Atlantiques* (n 1284), para 28.

1295 cf inter alia, the judgments in Case C-277/11 *M. M. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* [2012] OJ C 26/9, para 87 and case-law cited, and *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* (n 1293), para 46.

1296 *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* (n 1293), paras 40 and 41.

protected, the purpose of that rule is to allow them to correct any errors or submit information about their personal circumstances. This information can support either the adoption or non-adoption of the decision, or influence its specific content.[1297] That right also requires the authorities to pay due attention to the observations thus submitted by the person concerned, examining carefully and impartially all the relevant aspects of the individual case, and giving a detailed statement of reasons for their decision.[1298] The obligation to provide sufficiently specific and concrete reasons for a decision is a corollary of the principle of respect for the rights of the defence. This requirement ensures that the person concerned understands why their application is being rejected.[1299] In accordance with the Court's case law, observance of the right to be heard is required even where the applicable legislation does not expressly provide for such a procedural requirement.[1300] Thus, when the authorities of the Member States take measures which come within the scope of EU law, they are, as a rule, subject to the obligation to observe the rights of defence of addressees of decisions that significantly affect their interests.[1301] Where EU law does not specify the conditions for ensuring the rights of defence for illegally staying third-country nationals, nor the consequences of infringing those rights, national law applies. However, this is contingent on two principles. First, the rules established must be equivalent to those applicable to individuals in comparable situations under national law. Second, these rules should not make it practically impossible or excessively difficult to exercise the rights

1297 *Khaled Boudjlida v Préfet des Pyrénées-Atlantiques* (n 1284), para 37, referencing the judgments in Case C-349/07 *Sopropé — Organizações de Calçado Lda v Fazenda Pública* [2009] OJ C 44/16, para 49, and *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* (n 1293), para 47.

1298 cf the judgments in Case C-269/90 *Technische Universität München v Hauptzollamt München-Mitte* [1991] ECR I-5469, para 14 and *Sopropé — Organizações de Calçado Lda v Fazenda Pública* (n 1297), para 50.

1299 *Khaled Boudjlida v Préfet des Pyrénées-Atlantiques* (n 1284), para 38, with reference to the judgment in *M. M. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* (n 1295), para 88.

1300 Ibid, para 39, with reference to the judgments in *Sopropé — Organizações de Calçado Lda v Fazenda Pública* (n 1297), para 38, *M. M. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* (n 1295), para 86 and Case C-383/13 PPU - *M. G., N. R. v Staatssecretaris van Veiligheid en Justitie* [2013] OJ C 325/8, para 32.

1301 ibid para para 40, with reference to the judgment in *M. G., N. R. v Staatssecretaris van Veiligheid en Justitie* (n 1300), para 35.

conferred by the EU legal order.[1302] Those requirements of equivalence and effectiveness embody the general obligation of the Member States to ensure respect for the rights of defence that an individual derives from EU law, in particular as pertains to the definition of detailed procedural rules[1303] The Court noted that, according to its established case law, fundamental rights such as the rights of defence are not absolute. These rights can be restricted, but only under specific conditions. The restrictions must align with objectives of general interest pursued by the relevant measure. Additionally, they should not result in a disproportionate or intolerable interference that undermines the essence of the guaranteed rights.[1304]
The Court stated that the right to be heard does not obligate the relevant authority to notify an illegally staying third-country national before the interview about the possibility of adopting a return decision. Furthermore, the authority is not required to disclose the evidence it intends to use to justify that decision. That third-country national must have the opportunity effectively to submit his point of view on the subject of the illegality of his stay and reasons which might, under national law, justify that authority refraining from adopting a return decision.[1305] However, as noted by Advocate General Wathelet, an exception must be recognised. This applies when a third-country national could not reasonably suspect what evidence might be used against them. Additionally, the individual may only be able to respond to that evidence after certain checks or steps have been taken, particularly in order to obtain supporting documents.[1306]

With regard to the security flag, this means that the data subject must be heard in each case where the authority has added a security flag, before such a flag leads to consequences for the data subject; and they must be able to argue against the assessment of the authority. In cases where data subjects cannot reasonably suspect what evidence may be used against them, or where they can only respond to it after further checks, the evidence that the

1302 ibid, para para 41, with reference to the judgment in *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* (n 1293), para 51 and case-law cited.
1303 ibid, para para 42, with reference to the judgment in *Sophie Mukarubega v Préfet de police, Préfet de la Seine-Saint-Denis* (n 1293), para 52 and case-law cited.
1304 ibid para para 43, with reference to the judgments in Joined Cases C-317/08 to C-320/08 *Rosalba Alassini and Others v Telecom Italia SpA and Multiservice Srl v Telecom Italia SpA* [2010] OJ C 134/3, para 63, *M. G., N. R. v Staatssecretaris van Veiligheid en Justitie* (n 1300), para 33 and Case C-418/11 *TEXDATA Software GmbH* [2013] OJ C 344/10, para 84.
1305 ibid, para 55.
1306 ibid, para 56.

authority intends to rely on to justify its decision must be disclosed to them. This will be most cases, as data subjects do not know, in general, that their data are stored in an an Interpol, Europol or national security database. This is similar to criminal proceedings where, generally, the right to an adversarial hearing means that prosecution authorities should disclose to the defence evidence in their possession for or against the accused,[1307] as long as there are not grounds for limiting access, such as national security.[1308] It is argued here that at least the evidence that authorities have gathered to claim that a person is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in the Terrorism Directive or in any of the offences referred to in EAW Council Framework Decision,"[1309] has to be disclosed. Disclosure of such evidence, as has been discussed in the last chapter, will in most cases not carry a risk for national security or other grounds for limitations. The data subject also has to be heard on the outcome of the data comparison that triggered the security hit in the first place. Information on how a hit was triggered, as well as the personal data and details held in the database that triggered it, may only be limited to what is strictly necessary. In any case, the essence of the grounds for a decision must be disclosed.[1310] The authorities must give due weight to the observations submitted by the data subject, examining impartially and with careful consideration all relevant aspects of the individual case and providing a detailed statement of reasons for their decision. Only on that basis will the data subject have an effective right to request rectification or completion of particular personal data or information, and in certain cases to seek the deletion of a security flag.

Regarding the erasure of a security flag, Art. 17(4) Eurodac Regulation states that the Member State of origin must delete the record of the security flag from the dataset, if that Member State concludes that the threat to internal security no longer applies. Additionally, the Member State must consult any other Member States that have registered a dataset for the same person. Eurodac must inform the Member States of origin about the deletion of the security flag as soon as possible, and no later than 72 hours after another Member State of origin, which produced a hit, has completed

1307 *Rowe and Davis v the United Kingdom* (n 1093).

1308 *Edwards v the United Kingdom* [1992] 15 EHRR 417. In this case, the omission was held to have been rectified by the appeal process; cf also *Chahal and Others v United Kingdom* [1996] ECHR 1996-V.

1309 Eurodac Regulation 2024, Art 17(2)(i) and Recital 8.

1310 *ZZ v Secretary of State for the Home Department* (n 559), para 69.

the deletion. These Member States of origin are also required to delete the security flag in their corresponding datasets.[1311]

The Eurodac Regulation does not specify when restrictions on data processing must be imposed. However, the principle of accuracy in Art. 5(1)(d) GDPR requires the controller to process only data that are factually accurate and up to date.[1312] They are therefore required to verify contested data, both under this principle and pursuant to the right of rectification. In order to prevent possibly inaccurate data from continuing to be processed during this period, the data subject has a right to restriction of processing according to Art. 18(1)(a) GDPR.[1313] This means that if a data subject challenges a security flag and requests restriction of processing, other authorities would not be able to access the security flag and corresponding information during the rectification or erasure procedure.

A key question is whether a data subject may request the erasure only of the security flag itself, or also of the underlying information on which the flag is based. Two situations can be distinguished: first, a data subject may accept the underlying information but dispute the conclusion that they constitute a security threat.[1314] This will be the case if a data subject does not contest the data match resulting from the security check under Art. 15 Screening Regulation that triggered the security-related hit, but disputes that one of the additional requirements in Art. 17 Eurodac Regulation – for example, that they are considered violent – is met. If a court agrees with the data subject, the security flag will be deleted (and likely the information gathered to prove that the data subject is violent). The data match that triggered the hit in the first place may remain, as it is accurate. The situation differs, however, in a second scenario: a data subject may argue that the match itself is incorrect, or that the underlying entry in another database –

1311 Eurodac Regulation 2024, Art 17(4).

1312 Alexander Dix, 'Article 5 - Principles Relating to Processing of Personal Data' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection regulation: Article-by-Article Commentary* (Nomos 2023), para 100ff; Roßnagel, 'Artikel 5 - Grundsätze Für Die Verarbeitung Personenbezogener Daten' (n 521), para 4; Tobias Herbst, 'Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020), para 137.

1313 Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 34; Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 17; Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), para 13.

1314 As we will see below, rectification can only be requested for information that led to the conclusion that someone is a threat, not for the conclusion itself.

such as a Interpol or national security database – that produced the hit is inaccurate. In such cases, the data subject may seek not only the erasure of the security flag but also the correction or deletion of the underlying data entry that generated it. Based on the Eurodac Regulation, it is not possible to request the erasure of data governed by other legal frameworks, such as national intelligence or data protection laws. In practice, this often necessitates parallel proceedings. To ensure effective access to justice in such cases data subjects must have effective access to legal representation. This is particularly important in cases where the data subject faces difficulties in providing evidence to support the erasure of a security flag. Such situations are especially relevant when access to information is limited or when only minimal evidence exists – for example, when an assessment that a person is 'violent' is based solely on a single individual's statement, with no witnesses other than the data subject and that individual.

ddd) *Data Retrieved from Eurodac*

As discussed in the chapter on access to personal data and information, access to logs and records regarding which authority accessed Eurodac data is highly restricted. Also, it is unclear whether data subjects will be informed of the access to their data by law enforcement authorities, third countries, and other authorities.[1315] In practice, data subjects are unlikely to be able to fully track which authorities have accessed their Eurodac data. Consequently, even after a request for rectification, completion, erasure, or restriction of processing has been approved and the corresponding changes in Eurodac have been made, data subjects may not always know whether their data was accessed prior to these changes. As a result, they are unable to ensure that all authorities that have accessed their data have applied or acknowledged the updates. What is more, there is no provision in the Eurodac or the Interoperability Regulation that guarantees that changes made in these databases are communicated to authorities who accessed and/or retrieved data. The Eurodac Regulation also does not require that a record in the form of a written document be created and made available to the supervisory authority for requests related to rectification, completion,

1315 Chapter: The Right to Information.

erasure, or restriction of processing[1316] – unlike for access requests, where documentation is mandatory.

There is one provision that, to some degree, guarantees accuracy of data retrieved from Eurodac. Art. 47(4) Eurodac Regulation states with regard to personal data for law enforcement purposes that "[…] personal data, […], shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol".[1317] This provision ensures that Eurodac data retrieved for law enforcement purposes must not be recorded for more than a month outside of the Eurodac system, unless a criminal investigation is ongoing. What qualifies as an ongoing investigation will be discussed later. The provision does not entail a mechanism or procedure that ensures that changes in Eurodac are forwarded to the law enforcement authorities undertaking this ongoing investigation. Also, there is no mechanism that will guarantee that Member States and Europol erase personal data in due time.[1318]

The same applies to data shared with a third country following a hit obtained for law enforcement purposes. This data can be transferred if there is no "real risk" that the data subject may face a violation of their fundamental rights as a result of the transfer.[1319] There is no obligation stated in the Eurodac Regulation that if such data were rectified, completed or erased,

1316 Eurodac Regulation 2024, Art 43(8) *e contrario*.

1317 With regard to other search records, ibid, Art 41(4), holds "The records referred to in paragraph 1 of this Article may be used only for the data protection monitoring of the admissibility of data processing and to ensure data security pursuant to Article 46. Those records shall be protected by appropriate measures against unauthorised access and erased after a period of one year after the storage period referred to in Article 29 has expired, unless they are required for monitoring procedures which have already begun."

1318 With regard to the transmission of data between Member States ibid, Art 38(5) stipulates that "information received from Eurodac relating to other data found to be unreliable shall be erased as soon as the unreliability of the data is established." With regard to data security, ibid, Art 48(2)(h) states that Member States have to "ensure that all authorities with a right of access to Eurodac create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data, and make those profiles and any other relevant information which those authorities might require for supervisory purposes available to the supervisory authorities referred to in GDPR, Art 51 and in Police Directive, Art 41, without delay, at their request (personnel profiles)."; cf also Hartmut, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (n 73) 104ff.

1319 Recast Eurodac Proposal, Art 49(2).

this will be communicated to the third country. Even worse, the Eurodac Regulation does not state that third countries will have to erase such data after a certain period of time or at all.[1320]

According to the ECtHR, in its case Cemalettin Canlı, not only the keeping of false, inaccurate information but also the communication of incomplete information amounts to interference with the right to respect for a subject's private life.[1321] Art. 19 GDPR furthermore contains an obligation for the controller to notify the rectifications carried out to all the recipients of the data concerned.[1322] This obligation to forward justified rectifications or additions to previous data recipients prevents multiple separate requests from the data subject and helps limit the spread of erroneous information.[1323] The Eurodac Regulation does not make reference to this provision. It states that the rights in Art. 43 Eurodac Regulation should be exercised in accordance with Chapter III of the GDPR, to which Art. 19 belongs and forms *lex generalis*.

From an access to justice perspective, non-application of Art. 19 GDPR would appear problematic. If a data subject is not informed when their data are accessed and logs are unavailable through an access request, Member States must otherwise ensure transparency regarding rectification or erasure of personal data, even if retrieved from Eurodac. The written confirmation under Art. 43(3) Eurodac Regulation, which notifies the data subject of actions taken, should indicate who accessed the data and which authorities have been informed of the rectification or erasure. Nonetheless, data subjects may remain unaware of certain transfers to third countries or access by law enforcement authorities.[1324] Accordingly, they will likely not receive notification regarding these recipients.

1320 Data subjects, if they know about the use of incorrect data may request of the third country, to rectify or erase inaccurate data about them. If this third country, however, does now allow for this, or does not provide a law to this regard, the question is, whether the Eurodac Regulation may apply extraterritorially.

1321 *Cemalettin Canlı v Turkey* (n 1211), paras 41 - 42.

1322 cf GDPR, Art 17(2), which states that where information was made public, controllers "[…] shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

1323 de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 474.

1324 See chapters: The Right to Information, and The Right to Access Personal Data and Information.

eee) *Completion of Data Sets*

Rectification, or better, completion of a data set, often entails proving the absence of certain data. This may be straightforward in cases where, for example, a second name is missing from Eurodac, perhaps because the data subject travelled without documentation and was not asked about it during their interview. A middle name can later be added once the data subject provides valid evidence, such as a birth certificate. Completion is particularly crucial in large-scale information systems, where misidentification among individuals with the same name or date of birth is a risk. However, both completion and correction can be challenging if valid documents are unavailable or not recognised by a Member State.

Proving the absence of data can be considerably more challenging in other scenarios. For instance, this may occur when a data subject was not registered in a Member State despite being required to be. Consider a person seeking international protection in Greece who was not registered and later attempts to travel to Germany but is apprehended by police in Hungary. Upon checking Eurodac, the Hungarian authorities will find no entry. Nevertheless, the data subject may wish to be returned to Greece rather than have their asylum case processed in Hungary. Theoretically, the data subject should be able to have the data indicating 'place and date of the application of international protection' rectified.[1325] However, the principle of mutual trust requires that Member States generally assume that other Member States have respected the fundamental rights of the data subject and properly registered their asylum application.[1326] This trust may still apply when Member States inquire about the countries a person has traveled through[1327], and the data subject can provide supporting evidence, such as photographs, receipts, or transport tickets. Despite such proof, the data subject would be recorded as having applied for asylum in Hungary, not Greece. Any request to complete an entry that was not made in another Member State would have to be referred to that hypothetical Member State of origin – in this case, Greece.[1328] In practice, the Member State – *in casu* Hungary – will at best issue a take-back request.[1329] It will then be up to the

1325 Eurodac Regulation 2024, Art 17(1)(g).
1326 Chapter: The Right to an Effective Remedy.
1327 cf Silvia Cravesana and Maria Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (UNHCR 2017).
1328 Eurodac Regulation 2024, Art 43(2).
1329 AMMR, Art 40.

other Member State to accept the request, and the data subject's evidence will likely have minimal influence on the decision if no Eurodac entry exists.[1330]

bb) Interoperability Regulation

Asylum procedures are particularly prone to generating inaccurate data, especially when conducted under time pressure or in challenging circumstances, such as without professional translators, legal representatives, or confirmation that asylum seekers fully understood the process. Interoperability is likely to multiply these errors.[1331] Art. 48 Interoperability Regulation establishes the right to access, rectify, and erase data stored in the MID, as well as to restrict its processing with reference to the GDPR.

aaa) *Data in the CIR and sBMS*

Art. 48 Interoperability Regulations do not apply to data stored in the CIR or sBMS but only refer to the MID.[1332] In practice, an error in the MID will typically be based on inaccurate data in the CIR and sBMS. In the MID, links between different data sets are created in an automated process for the purpose of multiple-identity detection.[1333] The MID stores identity

1330 It might be noted that voluntary transfers are not available in some Member States nor is there any promotion of availing of this option in practice according to Cravesana and Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (n 1327) 148, fn 734, as reported in Denmark, Germany and Greece. In these states the data subjects will only be transferred, once the other Member State approves the take-back request (or the completion request). However, voluntary transfers are possible in some Member States if the applicant cooperates with the transfer, ibid 148, fn 736, as reported in France, Norway and Poland. Coming from such a country, the data subject might be able to travel while its request is still pending.

1331 see Paul Trauttmansdorff, 'The fabrication of a necessary policy fiction: the interoperability 'solution' for biometric borders' (2025) 12(2) Big Data & Society; FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 50; Matthias Leese and Fintan Marugg, 'Data Quality in European Law Enforcement and Border Control Cooperation: Findings from Survey Research' (ETH Zurich 2023).

1332 See chapter: The Right to Access Personal Data and Information.

1333 Interoperability Regulation - Judicial Cooperation, Art 25ff; Interoperability Regulation - Borders, Art 25ff.

confirmation files, containing links between data in the EU information systems included in the CIR and SIS.[1334] Both systems use the sBMS if biometric data are contained in the underlying information systems.[1335] Therefore, the rectification of data in the MID, i.e., the links between data in EU information systems, will frequently require a correction of the data stored in the CIR and/or in the sBMS. Otherwise, after the deletion of a link, a new one would occur between the same data sets.

As under the Interoperability Regulation only data in the MID can be rectified or erased, any information stored in the CIR or sBMS must be addressed through a request under the GDPR.[1336] Otherwise, rectification must be sought directly in the underlying databases supplying data to the CIR, such as Eurodac. This is, obviously, only possible if the data subject knows which database contains the erroneous data. The Interoperability systems, the MID,[1337] sBMS[1338] or the CIR,[1339] include a reference to the relevant information system. The data subject will, after having requested access to the references of the information systems holding their data, and rectification or erasure in the MID, need to seek rectification or deletion in the information system(s) that caused the erroneous link. This will necessarily lead to delays and complicate the procedure. FRA deems this "highly fragmented way to exercise the right to correction and deletion [...] ineffective."[1340] And indeed it is. From an access to justice perspective, it makes no sense to require the data subject to issue several rectification requests within interoperable systems.

1334 ibid, Art 25(1).
1335 ibid, Art 27(2).
1336 Chapter: The Right to Access Personal Data and Information. This means, that the data subject would have to submit their request to the controller according to GDPR, Art 16 and 17. According to Interoperability Regulation - Judicial Cooperation, Art 40, the controller of the data in the CIR remains the Member State authority that is the controller of the data in Eurodac, VIS, the EES, ETIAS and ECRIS-TCN. This means several dozen authorities across the Member States. It will not be easy for the data subject to find out which Member State to approach and within it, which authority.
1337 Interoperability Regulation - Judicial Cooperation, Art 25(2) in conjunction with ibid, Art 34; Interoperability Regulation - Borders, Art 25(2) in conjunction with ibid, Art 34.
1338 Interoperability Regulation - Judicial Cooperation, Art 13(2).
1339 ibid, Art 18(2).
1340 FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 50.

bbb) *Logs and Data Retrieved from the Interoperability Systems*

The Interoperability Regulations do not contain a provision that states a right to access logs kept by eu-LISA of the data processing operations, the MID,[1341] the sBMS,[1342] the ESP,[1343] and the CIR.[1344,1345] Similarly, the Interoperability Regulations do not provide data subjects with access to logs of the MID and CIR maintained at the national level.[1346] Furthermore, eu-LISA only stores logs of the processing operations. Logs showing which authority and which persons had access to certain data, on the other hand, may only be stored at the national level.[1347] Identifying recipients will make it necessary to combine the log files at the EU and Member States' level. This specific (over-)complexity leads to the risk that the identification may fail.[1348] For data subjects, this also means that they cannot track which authorities or persons accessed their data and whether they have rectified or erased data retrieved from the interoperability system, after it was deemed erroneous, or stored contrary to the law. The Interoperability Regulations do, however, in Art. 48 Interoperability Regulation and with reference to Art. 19 GDPR, contain a provision that guarantees that all authorities who have accessed data are notified of the obligation to rectify or erase it. Even though the subjective right of the data subject is limited, there is an obligation to communicate changes, at least with regard to the MID.

1341 Interoperability Regulation - Judicial Cooperation, Art 36; Interoperability Regulation - Borders, Art 36.
1342 ibid, Art 16(1).
1343 ibid, Art 10(1).
1344 ibid, Art 25(1).
1345 As regards the keeping of logs, ibid Art 10, 16 and 24 aim at framing the purposes for which logs may be used, as well as the retention period for these logs.
1346 ibid, Art 24(5) and 36(2); cf EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (n 646), no 133ff; ibid, no 136: "The EDPS therefore recommends to store the logs of the ESP and the shared BMS also at national level, as are the logs of the CIR (Article 24(5)) and the MID (Article 36(2))."
1347 Interoperability Regulation - Judicial Cooperation, Art 10, 16, 25 and 34; cf Curtin and Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55).
1348 Hartmut 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (n 73) 103.

ccc) *Links Indicating Deleted Data*

The Art. 29 Data Protection Working Party pointed out that white or red links created in the MID may lead to a prolonged retention period of data in the CIR, not foreseen by the law. Art. 23(2) Interoperability Regulations provides that the individual file – the data originating from the underlying information systems and white or red links created by the MID – shall be stored in the CIR for as long as the corresponding data are stored in at least one of the information systems. This provision seems to result in a longer period of retention of the data: if the red or white link stored in the CIR contains in itself the mention that it was created on the basis of data which originated from an underlying system where the data have been erased, in accordance with their retention period, this amounts to retaining the data for a longer period in the CIR.[1349] Whether this is lawful would need to be clarified through a request to delete the link. Accordingly, it should be possible to submit a request for their erasure. However, erasure requests are only permissible for data in the MID. The provision that could serve as a basis for such a request concerns the retention periods in the CIR, making it unclear whether it constitutes a valid ground for erasure in the MID.

c) *How to Rectify, Complete, Erase or Restrict Processing of Personal Data: Grounds for a Request*

With regard to how a request to rectify, complete, erase, or restrict the processing of personal data in Eurodac must be submitted, reference can be made to the corresponding section in the chapter on the right of access to personal data and information. Some additional points are warranted here, as requests for rectification, completion, erasure, or restriction differ in certain respects from access requests.

The Eurodac Regulation and the Interoperability Regulation provide that a request for rectification and erasure can be made in each or any Member State.[1350] The Member State to which a request has been made is responsible for ensuring that the Member State responsible for processing

1349 Art. 29 WP 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 19.

1350 Eurodac Regulation 2024, Art 43(2); Interoperability Regulation - Judicial Cooperation, Art 48(3).

the request receives it. The responsible Member State must subsequently rectify, complete, erase, or restrict processing of personal data, if necessary, and notify the data subject accordingly.[1351]

The main difference between an access request and a request to rectify, complete, erase, or restrict the processing of personal data is that the latter must include reasons. The data subject must specify which data they seek to correct, complete, erase, or restrict and provide justification for why the data are incorrect, incomplete, or why processing should be limited. This section will therefore examine the grounds for rectification, completion, erasure, or restriction of data under the Eurodac and Interoperability Regulations.

aa) Eurodac Regulation

aaa) *Inaccurate Data*

Data recorded in Eurodac that are "factually inaccurate" can be rectified.[1352] What factually inaccurate data means is not specified in the Eurodac Regulation. This can, from a technical point of view, be quite complex.[1353] Data can, for example, be of poor quality and still be accurate but lead to false hits or false non-hits.[1354] In order for the data sets to be accepted by the Eurodac Central System, the transactions and the fingerprint data sets sent should be of sufficient quality and in line with the Interface Control Document (ICD) that sets out the rules for data exchange between the Member States and the Central System.[1355] Fingerprint data sets should be

1351 Eurodac Regulation 2024, Art 43(2), (3); Interoperability Regulation - Judicial Cooperation, Art 48(3).

1352 Eurodac Regulation 2024, Art 43(4).

1353 cf Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (n 35); Sabina Leonelli and Niccolò Tempini (eds), *Data Journeys in the Sciences* (Springer Cham 2020); Robin Feldmann, 'Considerations on the Emerging Implementation of Biometric Technology' (2003) 25 Hastings Communications and Entertainment Law Journal 653; Dragana Kaurin, 'Data Protection and Digital Agency for Refugees' (World Refugee Council 2019); also Leese 'Between control and empowerment: Data quality in border and migration management' (n 64).

1354 cf Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (n 35).

1355 eu-LISA 'Eurodac 2022 Annual Report' (n 1194) 24; also: 2020 Eurodac Proposal, 58.

rejected in case of insufficient quality or sequence check failures, as they cannot be used for comparisons. Nevertheless, FRA field research revealed incidents of Dublin transfers being carried out based on false biometric matches.[1356] In the legal context of the GDPR, inaccuracy is described as an objective criterion and means that the information stored about the data subject does not correspond to reality. Inaccuracy can therefore only be used to describe statements of fact, not of value judgements.[1357] In a request for rectification, the data subject must identify which personal data do not correspond to reality and are factually inaccurate. This has specific implications for rectification requests concerning security flags. Since the determination that someone poses a security threat constitutes a value judgment, rectification can only be sought for the underlying information that led to this conclusion, not for the conclusion itself.

It is not relevant whether data were already incorrect when they were stored, or whether the incorrectness occurred later. In both cases, the data should be rectified. In some cases, inaccurate data have to be amended instead of rectified. This is particularly true if there is a duty to document, like in a medical record.[1358] The Eurodac Regulation explicitly states a right to complete data.[1359] Whether stored data are considered to be incomplete is determined by the data's respective processing purposes.[1360] Accordingly, data that were collected for a specific processing purpose may turn out to be incomplete when the processing purpose is changed (to the extent that such a change is permissible).[1361]

The inaccuracy of data does not have to relate to 'important' data. The right to rectification does not require proof that the inaccuracy has an adverse effect on the data subject; even insignificant or trivial inaccuracies

1356 FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 15.

1357 Alexander Dix, 'Article 16 - Right to Rectification' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection Regulation: Article-by-Article Commentary* (Nomos 2023), para 10; Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), para 11; Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 11; Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 8 and more on this dispute in para 9ff.

1358 Dix, 'Article 16 - Right to Rectification' (n 1357), para 6; Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 19: In this context, the right to file completeness must be observed ('Aktenvollständigkeit'); Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 8.

1359 Eurodac Regulation 2024, Art 43.

1360 de Terwangne, 'Article 16 - Right to Rectification' (n 1203) 473.

1361 Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 26.

result in a right to rectification.[1362] This is particularly noteworthy as, concerning Eurodac, the right to rectification is sometimes denied due to mutual trust. Third party information about the data subject also must be rectified if it is inaccurate.[1363] This seems especially important in the context of the security flag, which might rely heavily on third-party information. A Member State cannot rectify, by itself, data that have been transmitted by another Member State, according to Art. 43(2) Eurodac Regulation. They will contact the other Member State to check the accuracy of the data and the lawfulness of their transmission.[1364] Member States should do the same if data from a third party other than a Member State, such as Europol, are concerned. In the meantime, such data should be restricted for processing.

bbb) *Unlawfully Recorded Data*

Data logged in Eurodac that were "unlawfully recorded" must be erased.[1365] This means data that were collected in violation of the Eurodac Regulation have to be deleted. This is certainly true if, for example, data are collected from children under the age of six (although, in such a case, it might be possible that the child will turn six before an age assessment procedure is carried out, and its age proven). The most common infringement of a Eurodac provision is and will likely be the right to information. As discussed in the corresponding chapter, only some scholars accept that data may not be further processed when this right has been violated.[1366] In practice, however, this view is not followed: data in Eurodac are processed regardless of whether data subjects are aware of it or understand the purpose.
In addition, as discussed, security standards with regard to fingerprint matching have been lowered. Art. 38(4) Eurodac Regulation only provides for a fingerprint expert "where necessary". The obligation for a fingerprint expert to verify the results of a match, as stated in Art. 25(4) Eurodac

1362 Dix, 'Article 16 - Right to Rectification' (n 1357), para 8; Dix, 'Artikel 16 - Recht auf Berichtigung' (n 1229), para 11; Herbst, 'Artikel 16 - Recht auf Berichtigung' (n 1203), para 11.
1363 Dix, 'Artikel 16 - Recht Auf Berichtigung' (n 1229), para 13.
1364 Eurodac Regulation 2024, Art 43(2).
1365 ibid, Art 43(3); cf also GDPR, Recital 65.
1366 Dix, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 834), para 26; a different opinion is held by Bäcker, 'Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (n 522), para 65ff.

Regulation 603/2013, was not enforceable – at least according to a French court ruling. In a case in front of the Administrative Court of Appeal of Lyon (*Cour administrative d'appel*), the Court had to deal with the question of whether Art. 25(4) Eurodac Regulation 603/2013 regarding the verification of the match by a fingerprint expert, if breached, was serious enough to invalidate a transfer order. The Court stated that "[…] the sole purpose of this obligation is to guarantee the reliability of the results of the comparison, so that failure to comply with it cannot affect the regularity of the procedure followed where the reliability of the information resulting from the comparison is not seriously criticised."[1367] The data subjects had not done so and therefore the case was dismissed. It appears that, if no fingerprint expert is consulted, contrary to Art. 38(4) Eurodac Regulation, data will not be deleted, at least when the accuracy of the comparison result is not seriously questioned. However, such concerns should be raised in a request for erasure. The same might apply to cases where no expert is consulted for facial image hits, contrary to Art. 38(5) Eurodac Regulation.

In practice, it is likely that the violation of other (security-related) provisions in the Eurodac Regulation will ultimately not bear any consequences, at least not with regard to the question of erasure of "unlawfully recorded" data. Another example that points in this direction is that, despite the EU's promise to carry out a feasibility study on the use of facial images, this was never done.[1368] Similarly, the European Commission did not produce annual reports on access to Eurodac by law enforcement, contrary to its legal obligation under Art. 40(8) Eurodac Regulation 603/2013.[1369] It is possible that the right to erasure is interpreted quite restrictively, given the public interest in the storage and processing of data within Eurodac.

1367 CAA de Lyon, 18LY01453 (n 855), para 8.

1368 2016 Eurodac Proposal, 'Explanatory Memorandum' 4 states: "It is also proposed that an additional biometric – a facial image - will also be collected by Member States and stored in the Central System as well as other personal data to reduce the need for additional communication infrastructure between Member States to share information on irregular migrants that have not claimed asylum. The collection of facial images will be the pre-cursor to introducing facial recognition software in the future and will bring EURODAC in line with the other systems such as the Entry/Exit System. eu-LISA should first conduct a study on facial recognition software that evaluates its accuracy and reliability prior to this software being added to the Central System."

1369 'Jahresbericht über den Zugang der Gefahrenabwehr- und Strafverfolgungsbehörden zu Eurodac - Anfrage an: Europäische Kommission' (n 1197).

ccc) *Retention Periods*

The main ground for erasure of data is the fixed deadlines set by the Eurodac Regulation, after which data stored in Eurodac must automatically be deleted.[1370] Each set of data relating to an applicant for international protection is stored in Eurodac for ten years from the date on which biometric data were transmitted.[1371] Sets of data relating to other data subjects are stored in Eurodac for five years from the transmission date,[1372] with these exceptions: data subjects in Union resettlement frameworks who are not granted international protection or humanitarian status, whose data are recorded for three years;[1373] and beneficiaries of temporary protection, whose data are stored for one year.[1374] Upon expiry of the data storage periods, Eurodac automatically has to erase the data.[1375] Data relating to a person who has acquired citizenship of any Member State before expiry of this period have to be erased from Eurodac as soon as the Member State of origin becomes aware of it.[1376]

These varying retention periods categorise asylum seekers into different classes of data subjects, subject to greater or lesser restrictions with regard to their data rights. This differentiation in status has rightly been critisised.[1377] The long retention periods have also drawn scrutiny, particularly concerning children, who are recorded in Eurodac from the age of six.[1378] Biometric data from children is considered not to be fully reliable, as will be examined later.[1379] Storing their data, especially if they are under the age of twelve, might lead to more complications instead of protecting

1370 Eurodac Regulation 2024, Art 29.
1371 ibid, Art 29(1).
1372 ibid, Art 29(3), (5 - 8).
1373 ibid, Art 29(4) in conjunction with ibid, Art 18(2)(b) or (c).
1374 Eurodac Regulation 2024, Art 29(2) in conjunction with ibid, Art 26(1).
1375 Eurodac Regulation 2024, Art 29(10).
1376 ibid, Art 30(1).
1377 See Mouzourakis 'More laws, less law: The European Union's New Pact on Migration and Asylum and the fragmentation of "asylum seeker"' (n 287).
1378 cf Vavoula, 'Focus on Eurodac: Disentangled from the "Package Approach" but Is It Fit to Fly?' (n 607); Bianca-Ioana Marcu, 'Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors' (n 822); Chloé Berthélémy, 'Eurodac Database Repurposed to Surveil Migrants' (n 1143).
1379 Chapter: The Right to an Effective Remedy.

them.[1380] The interoperability systems, CIR, MID, and sBMS, are linked to Eurodac. They are supposed to automatically erase data, which was deleted in Eurodac,[1381] as will be discussed below.
Neither the Eurodac nor the Interoperability Regulation provide that data subjects will be informed that their data have been automatically erased. If the data subject does not keep track of the storage period, they will not know when their data were (supposed to be) deleted.

ddd) *Not-Ongoing Investigations*

According to the principle of purpose limitation in Art. 5(1)(b) GDPR, the processing of data is only permissible for a specific purpose. If processing data is no longer necessary to achieve the intended purpose – for example, once that purpose has been fulfilled – the data must be erased. Insofar as a change of purpose is permissible,[1382] the cessation of the need for data processing with regard to the original purpose does not lead to an

1380 The protection of children was one of the reasons given for storing data of as young children as six years old, cf European Commission, 'Explanatory Memo on the Pact on Migration and Asylum' (2024).

1381 The CIR is part of the Eurodac system architecture (Eurodac Regulation 2024, Art 31(1)(c)), so if data is erased in Eurodac, it is automatically erased in the CIR; regarding the sBMS and MID see Interoperability Regulation - Judicial Cooperation, Art 15(1): "The data referred to in Article 13(1) and (2) shall be stored in the shared BMS only for as long as the corresponding biometric data are stored in the CIR or SIS. The data shall be erased from the shared BMS in an automated manner"; ibid, Art 35: "The identity confirmation files and the data in them, including the links, shall be stored in the MID only for as long as the linked data are stored in two or more EU information systems. They shall be erased from the MID in an automated manner".

1382 cf Herbst, 'Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden")' (n 1205), para 22: The prerequisite for a permissible change of purpose is first of all that a legal basis for the processing for the new purpose exists; this can be consent related to the new purpose and the new processing or a legal provision under Union or national law. In addition, the requirements for changes of purpose set out in GDPR, Art 5(1)(b) and Art 6(4) must be met. Accordingly, processing for a purpose other than the original purpose of collection is only permissible if this new purpose is compatible with the original purpose. GDPR, Art 6(4) lists criteria for verifying the compatibility of the new purpose with the original purpose.

obligation to erase; this would only be the case when the need to fulfil the new purpose ceases to exist.[1383]

These considerations give rise to an important exception to the retention periods stated above. According to Art. 47(4) Eurodac Regulation, Eurodac, the designated and verifying authorities, and Europol keep records of searches for law enforcement purposes for the purpose of permitting the national data protection authorities and the EDPS to monitor the compliance of data processing, including for the purpose of maintaining records to prepare annual reports. Other than for such purposes, personal data as well as the records of the searches must be erased in all national and Europol files after a period of one month. It is important that the Eurodac Regulation sets a tight deadline for how long data extracted from Eurodac and stored in national files for law enforcement purposes can be kept. The one-month period does not apply in cases where the data are required for the purposes of the specific "ongoing criminal investigation" for which they were requested by a Member State or by Europol.[1384] In case of an ongoing criminal investigation, Europol and national law enforcement authorities can keep the data they retrieved from Eurodac. An *e contrario* reading of this provision leads to the conclusion that Eurodac data used in criminal investigations that are not ongoing (anymore) must be erased.

The Eurodac Regulation does not provide a definition of what constitutes an 'ongoing criminal investigation', nor does it set a maximum time limit on how long the data may be stored. It is unclear whether the term 'ongoing criminal investigation' covers only criminal investigations in the sense of national criminal law, or also investigations concerning national security by an intelligence service. The term 'criminal' may imply that it is the former. However, the conditions for access to Eurodac data by law enforcement authorities in accordance with Art. 33 and 34 Eurodac Regulation may also be met by national security authorities: the 'prevention' of criminal offences, which is typically not done by police or prosecutors but by intelligence authorities, is also covered. Investigations by intelligence services may take

1383 ibid, para 21; similar Peuker, 'Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden")' (n 1210), para 17; Dix, 'Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden")' (n 1205), para 11.

1384 Eurodac Regulation 2024, Art 47(4).

an even longer time. They might be labelled as ongoing without the same specific requirements for actions as in criminal investigations.[1385]

Data subjects will likely remain unaware that their Eurodac data have been accessed, particularly in the context of intelligence investigations, and only learn of it in a criminal proceeding when all evidence must be disclosed to the suspect. General erasure requests would, moreover, typically apply only to police or intelligence databases, not Eurodac. Member States and Europol should thus indicate in their accountability reports (in anonymised form) which investigations with data obtained from Eurodac are ongoing.[1386] That way, national data protection authorities and the EDPS will have an overview of how long these data have been kept outside the Eurodac system. In this context, too, adhering to the notification obligation in Art. 19 GDPR seems crucial.

bb) Interoperability Regulation

aaa) *Data Quality*

As has been discussed above, rectification and erasure requests can, in the context of the interoperability systems, only be made with regard to the MID. A ground for requesting the deletion of a (red) link would be if the data subject disputes that the linked data sets both represent their personal data. Alternatively, the data subject may acknowledge that the data sets represent their personal data but argue that they do not represent 'multiple identities', only one and the same identity. In many cases, challenging a link will only be possible if there are concerns about the quality of the data used for the comparisons.

Data quality is a challenge when it comes to large-scale databases – especially in interoperable systems linked to several databases.[1387] The Implementing Regulation for the Interoperability Regulations by the Commission specifies automated data quality control mechanisms and procedures, common data quality indicators, and the minimum quality standards for

1385 The phase of criminal intelligence gathering prefaces a phase of criminal investigation, where charges must be filed at some point, or the case is closed. Cf UN Office on Drugs and Crime, 'Criminal Intelligence: Manual for Analysts' (2011).

1386 Eurodac Regulation 2024, Art 57(8).

1387 See chapter: The Right to an Effective Remedy.

storage of data in the Interoperability Systems.[1388] It states that data are categorised in different quality categories, which are: good quality, low quality, and rejected.[1389] "Data cleaning and issue detection mechanisms must regularly check the validity and the data quality compliance of the data stored in the EU information systems and interoperability components […]."[1390] Where the input data are assigned with a 'good quality' classification, the data shall be stored into the system or component without any data quality alert. However, the Regulation states that, "[w]here the input data is assigned with a 'low quality' classification, the data shall be stored into the system or component and with a data quality alert. An alert shall indicate that the input data shall be rectified and the reason why the input data does not demonstrate the required compliance with the applicable data quality indicators. Where possible, the alert shall identify the data field(s) or the data content(s) or both affected by data quality issues and suggest the changes necessary for the input data to meet the 'good quality' classification."

The Implementing Regulation does not clarify whether data subjects are informed about this, and who is able to see the 'low quality' alert. It is unclear whether, when data are marked with an alarm in the CIR, the same

1388 Commission Implementing Regulation (EU) 2021/2224 of 16 November 2021 Laying Down the Details of the Automated Data Quality Control Mechanisms and Procedures, the Common Data Quality Indicators and the Minimum Quality Standards for Storage of Data [2021] OJ L448/14 (Implementating Regulation 2021/2224).

1389 ibid, Annex, Section 3.

1390 ibid, Art 3(8); ibid, Annex, Section 4 furthermore specifies: "Two types of mechanisms shall be used for the purposes of Article 3(8): a) Data cleaning mechanisms. Such mechanisms shall carry out checks to identify data for which the remaining retention period is less than the time defined in the legislation governing the relevant EU information system or interoperability component. Data cleaning mechanisms shall inform the Member State of the scheduled erasure of the data and allow them to adopt, if necessary, the appropriate measures; b) Issue detection mechanisms. Such mechanisms shall carry out checks to identify the data that no longer meet one or more data quality rules or standards related to data quality indicators. Such checks may return an alert or notification to the responsible authority of the Member State indicating the reason why the data no longer meets one or more data quality rules or standards. Where possible, the alert shall suggest the changes necessary for the input data to meet the new rules or standards. In no case the application of such checks shall lead to automated deletion of data stored in the EU information systems or interoperability components. When new data is being entered into an EU information system or interoperability component while the issue detection mechanisms are running, the issue detection mechanisms shall not apply to those data."

marking appears in the respective underlying system. It is also uncertain whether all authorities with access to that system can see this marking. In any case, if a (red) link was made between data sets of which one does not show 'good quality', the data subject should be informed of this at least in cases where they deny the accuracy of the link. Such data should be rectified. Also, if authorities are able to see the 'low quality' alert in the underlying system, they will be aware that a rectification request regarding such data might likely have merit.

bbb) *Retention Periods*

The interoperability systems, the CIR, MID and sBMS, are linked to Eurodac and are supposed to automatically erase data, which was deleted in Eurodac.[1391] The Interoperability Regulation states that where data are added, amended, or deleted in Eurodac, the data stored in the individual file of the CIR has to be added, amended, or deleted accordingly in an automated manner.[1392] Furthermore, an individual file is intended to be retained in the CIR only for as long as the corresponding data exist in at least one of the EU information systems contributing data to the CIR.[1393] The sBMS only stores templates from data from the CIR and SIS, which have to be erased automatically, when the corresponding data in the CIR and SIS are erased.[1394] The identity confirmation files, together with their data and links, are to be stored in the MID only as long as the linked data exist in two or more EU information systems. Once this condition no longer applies, the data must be automatically erased from the MID.[1395] No notification of erasure has to be provided to the data subject. If a

1391 The CIR is part of the Eurodac system architecture (Eurodac Regulation 2024, Art 3(1)(c)), so if data is erased in Eurodac, it is automatically erased in the CIR; regarding the sBMS and MID see Interoperability Regulation - Judicial Cooperation, Art 15(1): "The data referred to in Article 13(1) and (2) shall be stored in the shared BMS only for as long as the corresponding biometric data are stored in the CIR or SIS. The data shall be erased from the shared BMS in an automated manner"; ibid, Art 35: "The identity confirmation files and the data in them, including the links, shall be stored in the MID only for as long as the linked data are stored in two or more EU information systems. They shall be erased from the MID in an automated manner."

1392 Interoperability Regulation - Judicial Cooperation, Art 19(1).

1393 ibid, Art 23(2).

1394 ibid, Art 15.

1395 ibid, Art 35.

data subject becomes aware that their data are being retained beyond the prescribed retention period, they can request its erasure.

ccc) *The Web Portal and its Limits*

The Interoperability Regulations establish their own system for rectification and erasure requests. Under the Interoperability Regulations, rectification and erasure requests must be submitted in a web portal, according to Art. 49 Interoperability Regulations. Challenges related to the web portal have been discussed in the previous chapter; reference can be made to the analysis provided there.[1396]

cc) Standard of Proof

Important questions regarding the right to rectification, completion, erasure, and restriction of processing of data concern who bears the burden of proof, what the standard of proof is for demonstrating that data are erroneous, and what evidence the data subject must or can provide. The standard of proof is intrinsically linked to the right to an effective remedy; for this reason, further explanations on the burden and standard of proof concerning Eurodac hits and security flags are provided in the next chapter.

It should be kept in mind that no matter how "big" data are, the road from data to knowledge remains complex and full of obstacles.[1397] When large amounts of data are collected and processed, errors occur often. Especially a system like Eurodac is prone to errors: alphanumeric data of people who do not use the Latin alphabet is recorded in Latin letters; biographic data are stored from data subjects who do not carry birth certificates or passports; biometric data are taken under conditions that are in many cases far from ideal.[1398] These are merely some examples of the difficulties that can arise in the process of obtaining information from data. Numerous other challenges exist, including technical issues such as

1396 Chapter: The Right to Access Personal Data and Information.

1397 Leonelli and Tempini, *Data Journeys in the Sciences* (n 1353), v.

1398 Forti 'Addressing Algorithmic Errors in Data-Driven Border Control Procedures' (n 30) 639; FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674) 30.

errors in biometric matching or complications in data sharing between national and international systems.[1399] Existing EU information systems already exhibit a substantial number of inaccuracies in the data they contain. The Council of the EU admitted that "analyses have demonstrated that the quality of data in eu-LISA systems could, at least in some instances, be improved. Issues encountered include inappropriate use of data fields, data inconsistencies, use of incorrect data formats, insertion of records with missing data and insertion of poor-quality biometric samples".[1400] Such inaccuracies can have serious consequences for individuals, which risk to multiply with interoperability.[1401] Under the new Eurodac Regulation, much more biographic and new biometric data are stored. This makes the risk of storing even more inaccurate data even higher.[1402]

3. Rectification and Erasure in Practice: Accessibility, Justiciability and Consequences of a Violation

Unlike the right to information and the right of access to personal data, questions regarding the accuracy of Eurodac data and entries are occasionally addressed, including at the national level. However, as we will see, claims challenging the correctness of Eurodac data are often not thoroughly examined in practice. This section will first review figures and studies from EU agencies and international organisations relating to rectification and erasure issues in Eurodac. It will then explore European and national case

1399 Leese, 'Between control and empowerment: Data quality in border and migration management' (n 64) 6; for more cf Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (n 35); Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange At EU-Level* (n 542); Leonelli and Tempini, *Data Journeys in the Sciences* (n 1353); Elena Carpanelli and Nicole Lazzerini (eds), *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law* (Springer International Publishing 2019); Huub Dijstelbloem and Albert Meijer (eds), *Migration and the New Technological Borders of Europe* (Palgrave Macmillan UK 2011).

1400 13258/16 from Presidency, Council of the European Union, 'Renewed Information Management Strategy (IMS) – 5th Action List – State of Play' (14 October 2016).

1401 See Trauttmansdorff (n 1331); FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications' (n 71) 50; Leese and Marugg, 'Data Quality in European Law Enforcement and Border Control Cooperation: Findings from Survey Research' (n 1331).

1402 FRA 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 38.

law concerning the accessibility and justiciability of the rights to rectification, completion, and erasure of Eurodac data.

a) *Numbers*

eu-LISA publishes some numbers on Eurodac transactions, hits, and data stored in its annual report. This report does not entail figures on how many requests for rectification, completion, erasure, and restriction of processing were made. The only number shown in the report is access requests, which amounted to 342 in the year 2022. This was an increase from the years before: the lowest number was 97 in 2018, the highest 224 in 2021.[1403] Most requests for access to personal data came from Cyprus (202), followed by France (107), as was the case in the previous year.[1404] It can be concluded from these low numbers for access requests that the number of requests for rectification, completion, erasure and, restriction of processing of data is probably even lower.

Some idea of data accuracy can be gained from other numbers that are published by eu-LISA. In 2022, four Member States transmitted more than 10% of their Category 1 data sets with a delay of more than 72 hours. In 2021, there were eight such Member States. Ireland transmitted 28% of its Category 1 data to the Central System with a delay of more than 72 hours in 2022, followed by Portugal (21%), Switzerland (15%), and Latvia (10%). Those delays were responsible for 1,270 wrong Category 1 hits against Category 1 data sets in keeping with the trend in previous years.[1405]
Concerning Category 2 data sets, six Member States transmitted more than 10% of their data with a delay of more than 72 hours (five Member States in 2021). Sweden transmitted 50% of its Category 2 data with a delay of over 72 hours, followed by Malta (40%), Slovakia (33%), Poland (33%), Croatia (12%), and France (11%). Those delays in transmitting Category 2 data sets resulted in 614 missed hits in 2022. The vast majority of these were related to data transmitted by Croatia (502 hits), followed by Spain (58), Poland (20), and Italy (17).[1406]

1403 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 25. The reports for 2023 and 2024 had not been published by the time of the finalisation of this book.
1404 ibid 25.
1405 ibid 23ff.
1406 ibid 24.

As mentioned above, for a data sets to be accepted by the Eurodac Central System, the transactions and the fingerprint data sets sent should be of sufficient quality and in line with the ICD that sets out the rules for data exchange between the Member States and the Central System. Fingerprint data sets are rejected in case of insufficient quality or sequence check failures, as they cannot be used for comparisons. In 2022, the average rejection rate for fingerprint data sets was 3.11% (36,946 data sets were rejected, under Categories 1 and 2), representing a slight decrease in relative terms compared to the previous year, when the rejection rate was 3.98%.[1407] Transaction errors may occur due to data validation issues (incompatibility with the ICD) or incorrect formats. In 2022, 79,775 transactions (entries, updates and deletions) were rejected due to errors, accounting for 4.25% of all transactions. This was less than the year before, when a total of 112,407 transactions were rejected, accounting for 9.34% of all transactions.[1408]

These figures do not reveal the exact extent of incorrect data in Eurodac, but they indicate that the system is not flawless and that data quality is not always reliable. It can be expected that these issues will increase once the new Eurodac Regulation takes effect, as significantly more data will be stored. A similar trend is likely once interoperability becomes operational.

b) *Studies*

A 2017 UNHCR study on the implementation of the Dublin III Regulation examined the use of evidence in asylum, transfer, and return procedures, including the weight given to Eurodac data. This is particularly relevant for understanding whether indications or complaints about incorrect Eurodac data are addressed. It also raises questions about the practical enforceability of the right to rectification, especially when this right is exercised within the framework of an asylum, transfer, or return procedure rather than through a separate procedure.

According to UNHCR, some proof or evidence appears more easily accepted in asylum procedures than others. For instance, objective evidence of a fingerprint hit under Eurodac is more readily accepted compared to personal documents certifying a family relationship and the presence of

1407 ibid 24.
1408 ibid.

family members in another Member State.[1409] Generally, it appears that Eurodac and VIS evidence takes precedence; more weight is placed on it in evidentiary terms than other information provided by the applicant in relation to their journey. A Danish NGO surveyed cases and found that when a Eurodac or VIS hit occurs, personal interviews tend to focus on that hit rather than on family links or the applicability of other criteria under Chapter III of the Dublin III Regulation. An NGO in Italy reported that, as the personal interview is generally conducted in a superficial way, and some elements for applying certain criteria of the Dublin III Regulation might not emerge during it, the Eurodac or VIS-hits prevail in practice, prompting the application of certain criteria over others.[1410] Applicants in the UK expressed the view that the authorities prioritised fingerprints or the willingness of another Member State to take charge over and above any other forms of evidence. In France, the increase in applicants for international protection resulted in personal interviews held sometimes only after a request was submitted to another Member State on the basis of a Eurodac or VIS hit.[1411]

Due to the lack of detailed guidance or specific lists of evidence required to prove family links, inconsistent practices are reported in several Member States.[1412] There appears to be a flexible approach in some of these countries regarding what is considered acceptable evidence of family links.[1413]

The fact that Eurodac data are given so much evidentiary weight is not unproblematic. As seen above, the quality of such data is not always guaranteed. Much less weight is given to other evidence; this can be problematic, even in cases where Eurodac data are correct but provides an incomplete picture – e.g., when a person has already travelled through a Member State but has family in another country. Therefore, the latter would be responsible for processing an asylum application. It is even more difficult for an asylum seeker if Eurodac data are actually incorrect, because it may be more difficult to prove this. A lawyer interviewed in Sweden by FRA recalled several cases when asylum seekers ended up being transferred as Dublin cases: "I don't know how many. But, these are people who said

1409 Cravesana and Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (n 1327) 89.
1410 ibid 89.
1411 ibid.
1412 As reported in France, Germany, Italy and Malta.
1413 Cravesana and Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (n 1327) 90.

in a very sincere way, I HAVEN'T been there". The lawyer concluded that it is in principle impossible to challenge a biometric match made by the authorities.[1414]

Some scholars have taken the use of Eurodac in the practice of the Dublin system as a starting point to predict how Member States will handle data in the interoperability system: "Depending on the Member State, national authorities that access interoperable information systems may adopt quite different practices in how they deploy the data they retrieve. The use of Eurodac in the practice of the Dublin system is revealing. While some national authorities – like the Portuguese – seem to generally take the accuracy of the information they receive from their counterparts for granted, other national authorities – such as the Danish – rely more on other sources of evidence.[1415] Nevertheless, through interoperability, incorrect information entered into one particular information system is liable to contaminate others."[1416]

In addition to these studies on how much weight is given to Eurodac data as evidence, it must be taken into account that there are procedural hurdles that make it difficult to bring forward a request for rectification of Eurodac data. One issue is Art. 43(2) AMMR. It stipulates that Member States must allow a period of at least one week but no more than three weeks after notifying a transfer decision. During this time, the person concerned may exercise their right to an effective remedy. This very short time to appeal a transfer decision may infringe on the right to be heard and the effectiveness of the right to rectification – especially in cases where the period is set for one week. According to the ECtHR, an excessively short time limit for filing an application (for example, in fast-track asylum procedures) and/or for appealing against a subsequent removal (or transfer) decision may render the procedure ineffective in practice. It may thus be in breach of the requirements of Art. 13 ECHR taken together with Art. 3 ECHR.[1417] Remedies may prove effective if the asylum seeker is heard and enjoys safe-

1414 FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674) 32.

1415 The article makes reference here to DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (n 695).

1416 Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 67ff.

1417 ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), para 125, with reference to *I.M. v France* App no 9152/09 (ECtHR, 2 February 2012), paras 136 - 160; *R.D. v France* App no 34684/14 (ECtHR, 16 June 2016), paras 55 - 64.

guards for the purposes of making their case, in spite of tight deadlines.[1418] Considerations regarding short time limits for filing an application have also been made by the CJEU.[1419] What is more, the UNHCR found, in its study on the implementation of the Dublin III Regulation, that in three Member States, only the applicant is notified of a transfer decision, despite having a legal advisor legally representing them in the Dublin procedure. In two Member States, only the legal advisor is informed of the transfer decision, and it is their responsibility to inform the applicant. The transfer decision is normally notified directly after the responsible Member State accepts the take-back or take-charge request or within a few days of such acceptance.[1420] This can lead to miscommunication and a delay in lodging an appeal – which in turn makes it more difficult to gather and present evidence. A challenge also exists in Germany, whereby legal advisors are sometimes informed at a later stage than the applicants they represent. This also affects the ability of the applicant to submit an appeal in practice.[1421] Other states only notify about a transfer decision by post; homeless applicants will often know of the decision at a later stage, since they cannot or will not check the mail every day.[1422]

The considerable evidentiary weight given to Eurodac data, combined with procedural challenges such as short time limits, makes effective access to the right to rectification and erasure difficult. This is compounded, as will be discussed later, by the strong emphasis placed on the principle of mutual trust.

1418 *E.H. v France* App no 39126/18 (ECtHR, 22 July 2021), paras 174 - 207.

1419 cf Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.86ff; The CJEU has also held that, in respect of national legislation that comes within the scope of EU law, it is for the Member States to establish time limits in the light of, inter alia, ' the significance for the parties concerned of the decisions to be taken, the complexities of the procedures and of the legislation to be applied, the number of persons who may be affected and any other public or private interests which must be taken into consideration (Case C-651/19 *JP v Commissaire général aux réfugiés et aux apatrides* [2020] OJ C 378/15, para 53, referring to Case C-63/08 *Virginie Pontin v T-Comalux SA* [2009] OJ C 312/4, para 48.

1420 Cravesana and Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (n 1327) 142.

1421 ibid 142.

1422 ibid 144.

c) *European Case Law*

To date, there is no case from a European court that explicitly deals with the right to rectification and erasure in connection with Eurodac data. This section examines case law in the field of asylum law that offers relevant insights into the right to rectification and the right to erasure.

The ECJ has ruled that the data subjects should have the opportunity to submit information relevant to the determination of the Member State responsible for the processing of an asylum claim and have an effective remedy against a transfer decision. In Mehrdad Ghezelbash v Staatssecretaris van Veiligheid en Justitie, the ECJ stated that the EU legislature, through the Dublin III Regulation, decided to involve asylum seekers in the process of determining which Member State is responsible for their application.[1423] This is done by obliging Member States to inform them of the criteria for determining responsibility and to provide them with an opportunity to submit information relevant to the correct interpretation of those criteria, and by conferring on asylum seekers the right to an effective remedy in respect of any transfer decision that may be taken at the conclusion of that process.[1424] Pointing out erroneous Eurodac data can be such relevant information.

The Court also ruled that a transfer decision does not need to have an automatic suspensive effect. Yet, it must be possible under Art. 27 Dublin III Regulation (replaced by Art. 43 AMMR) to request the suspension. Only if this is not granted can a transfer decision be implemented.[1425] Suspension of a transfer decision should be granted if a person files a rectification request, until at least a decision on the merits of such a request has been issued.

In another case, X, the ECJ considered a request for a preliminary ruling regarding the right of an asylum applicant to submit evidence. In this a case fingerprints were taken from the applicant which was subsequently treated as him having requested asylum in that Member State.[1426] The data subject from Syria had agreed to his fingerprints being taken by Polish authorities under threat of refoulement to Belarus, on the advice of an organisation, unaware that that amounted to making an application for

1423 *Mehrdad Ghezelbash v Staatssecretaris van Veiligheid en Justitie* (n 840).
1424 ibid, para 51.
1425 ibid, para 59.
1426 Case C-392/22 *X v Staatssecretaris van Justitie en Veiligheid* [2024] 2024/195.

international protection.[1427] On that occasion, he had received documents in Polish and a document in Arabic containing information about the Dublin III Regulation but had not been assisted by an interpreter.[1428] The Court opined that it is apparent from Art. 5(2) Dublin III Regulation that the applicant must have the opportunity to "present all [...] information which is relevant to correctly determine the Member State responsible".[1429] The applicant must be able to provide any relevant elements of proof or any circumstantial evidence[1430] relating to the determination of the Member State responsible.[1431] The Court decided that any evidence provided by the applicant to establish a risk of treatment contrary to Art. 4 CFR must be considered. However, it is, according to the Court, the responsibility of the judicial authorities of the Member State tasked with determining which Member State is responsible to assess this evidence. They must evaluate it based on objective, reliable, specific, and properly updated information. Additionally, they must take into account the standard of protection of fundamental rights guaranteed by EU law to determine whether the alleged deficiencies actually exist.[1432] While this seems to give the data subject the possibility to request the rectification of Eurodac data, the judgment says nothing about what the probative value must be for such a claim to be heard and investigated. As we will see in the next case, in practice, the data subject not only has to provide evidence showing the incorrectness of data. The principle of mutual trust may override the right of the data subject.

1427 ibid, para 14.
1428 ibid.
1429 ibid, para 71.
1430 without the meaning of Dublin III Regulation, Art 22(2) and (3).
1431 *X v Staatssecretaris van Justitie en Veiligheid* (n 1426), para 72. The Court continues in ibid, para 73: "Furthermore, the Dublin III Regulation, Art 21(3), refers to those elements of proof or that circumstantial evidence, but also to relevant elements from the applicant's statement, enabling the authorities of the requested Member State to check whether it is responsible on the basis of the criteria laid down in that regulation." And *X v Staatssecretaris van Justitie en Veiligheid* (n 1426), para 74: "Lastly, Dublin III Regulation, Art 22(4) and (5) makes clear that the requirement of proof should not exceed what is necessary for the proper application of that regulation and that, if there is no formal proof, the requested Member State is to acknowledge its responsibility if the circumstantial evidence is coherent, verifiable and sufficiently detailed to establish responsibility."
1432 *X v Staatssecretaris van Justitie en Veiligheid* (n 1426), para 76, referencing, to that effect to Case C-163/17 *Abubacarr Jawo v Bundesrepublik Deutschland* [2019] OJ C 187/7, para 90, and *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), para 136.

The importance of the principle of mutual trust with regard to Eurodac data became clear in a case in front of the ECJ called Abdullahi. The case concerned an asylum seeker, Ms Abdullahi, who lodged an application for international protection in Austria with the Federal Asylum Office (*Bundesasylamt*), the competent authority. Ms Abdullahi had been travelling through several European countries, among them Greece and Hungary, without having been recorded in Eurodac. The Federal Asylum Office then requested that Hungary take charge of Ms Abdullahi. Hungary agreed to do so because – according to the information provided by Ms Abdullahi, as forwarded to Hungary by the Austrian Republic, and the general information available concerning the routes taken by illegal immigrants – there was sufficient evidence that Ms Abdullahi had entered Hungary illegally from Serbia and that she had subsequently travelled directly to Austria.[1433] A further appeal, brought months later before the Asylum Court (*Asylgerichtshof*), was lodged against that decision: Ms Abdullahi claimed that the Member State responsible for her asylum application was not Hungary but the Hellenic Republic, since she had been travelling through it. She argued that the Hellenic Republic did not observe human rights in certain respects and that, accordingly, it was up to the Austrian authorities to complete the examination of her asylum application.[1434]

The ECJ had to decide in which Member State Ms Abdullahi's asylum claim was lodged. The Court pointed out that the second Member State (Hungary) agreed to take charge of Ms Abdullahi,[1435] namely, as the Member State of Ms Abdullahi's first entry into EU territory. The Court determined that in a situation where a Member State agrees to take charge of an asylum applicant, the applicant can only challenge the choice of that Member State by citing systemic deficiencies in its asylum procedure. Additionally, the applicant can raise concerns about the conditions for receiving asylum applicants in that Member State. These deficiencies must provide substantial grounds for believing that the asylum applicant would face a real risk of being subjected to inhuman or degrading treatment, as defined by Art. 4 CFR.[1436]

What is interesting in this case is that the ECJ does not seem to deny that

1433 Case C-394/12 *Shamso Abdullahi v Bundesasylamt* [2013] OJ C 45/12, para 28.

1434 ibid, para 32.

1435 On the basis of the criterion laid down in Dublin II Regulation, Art 10(1).

1436 *Shamso Abdullahi v Bundesasylamt* (n 1433), para 60, with reference to that effect to Joined Cases C-411/10 and C-493/10 *N. S. v Secretary of State for the Home Department and M E and Others v Refugee Applications Commissioner and Minister*

Ms Abdullahi travelled through Greece – and in this respect that Eurodac data were not recorded correctly. However, this does not matter, according to the Court, because the principle of mutual trust prevails. This will also be evident in cases at national level.

d) *National Case Law*

No cases could be found in this study in which a data subject directly requested the correction, completion, erasure, or restriction of processing of Eurodac data based on the Eurodac Regulation. And cases regarding erroneous biometric matching are rare.[1437] There are cases in which the question of whether data in Eurodac or national databases are dealt with correctly. This issue frequently arises in cases where an asylum seeker claims to be a minor, despite being registered (until today in national databases, soon also in Eurodac) as an adult. It also occurs when an asylum seeker asserts that they have not applied for asylum in the Member State to which they are being returned. The following compilation of cases is intended to provide an overview of national case law regarding Eurodac data. It is, however, by far not an exhaustive overview and, as will be seen, does not cover many of the questions and constellations discussed above. As already mentioned, much less data have been stored under the old Eurodac Regulation 603/2013. This is why this overview does not show what questions can and will arise under the new Eurodac Regulation with regard to rectification and erasure requests. As a great deal of data on asylum seekers is already stored in national databases, it would be informative to examine how requests for rectification, completion, or erasure are handled there. However, this would go beyond the scope of this study but might be a source of arguments in future cases regarding Eurodac data.

Rectifying the Date of Birth

A category of case law that occurs repeatedly in practice is data subjects contesting the date of birth, which will be registered in Eurodac under

for Justice, Equality and Law Reform [2011] ECR I-13905, paras 94 and 106, and Case C-4/11 *Bundesrepublik Deutschland v Kaveh Puid* [2013] OJ C 9/2, para 30.

1437 There is one case concerning an asylum seeker in the UK, who was detained longer than lawfully permitted due to a false fingerprint match with another person England and Wales High Court (Administrative Court) - *Kamara v Secretary of State for the Home Department* [2013] EWHC 959.

Art. 17(1)(e) Eurodac Regulation. Problems around the date of birth have been known for a long time; incorrect registration of a minor's age is a common occurrence, particularly in periods of chaos, when large numbers of asylum seekers arrive. Sometimes, it is also due to miscommunication or a lack of information provided to minor asylum seekers.[1438] Furthermore, there are countries where many people do not know exactly when they were born. Thus, a hypothetical date of birth is assumed for the registration in Eurodac.[1439] For juveniles in asylum procedures, the date of birth is often questioned. In some cases, a procedure is carried out to determine the year of birth.[1440] An important problem with the subsequent rectification of the date of birth, or any other data for that matter, is that the principle of mutual trust may stand in the way of the right to rectification.

An example can be given of a Dutch case involving an Eritrean asylum seeker who, though a minor, was registered as an adult by the Italian

1438 cf Brouwer, 'Interoperability of Databases and Interstate Trust: A Perilous Combination for Fundamental Rights' (n 1180); Spaggiari, Thompson and Papangeli, 'How European Countries Wrongfully Classify Children Seeking Asylum as Adults' (n 817).

1439 For thousands of refugees from Syria, Afghanistan and other countries, 1 January is their birthday on their papers (Annette Kögel, 'Bürokratie in Berlin: Warum viele Geflüchtete Neujahrskinder sind' *Tagesspiegel* (1 January 2018) <https://www.tagesspiegel.de/berlin/warum-viele-gefluchtete-neujahrskinder-sind-8515381.html>). Asylum seekers from Afghanistan are not the only ones who often have January 1st as a birthday on their documents. The same is the case with citizens of other war-torn countries, like Syrians, Iraqis, Somalians, Sudanese, Ethiopians, and Vietnamese, according to Stavros Malichudis and Iliana Papangeli, 'Born on January 1st' *We Are Solomon* (25 April 2021) <https://wearesolomon.com/mag/focus-area/migration/born-on-january-1st/>).

1440 See for more on this, e.g., World Medical Association, 'WMA Statement on Medical Age Assessment of Unaccompanied Minor Asylum Seekers - Adopted by the 70th WMA General Assembly, Tbilisi, Georgia' (2019); Maria Antonia Di Maio, 'Position Paper on Age Assessment in the Context of Separated Children in Europe' (Separated Children in Europe Programme 2012); Bundesärztekammer, 'Stellungnahme der zentralen Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten (Zentrale Ethikkommission) bei der Bundesärztekammer - "Medizinische Altersschätzung bei unbegleiteten jungen Flüchtlingen"' (2016); German Medical Association's Central Ethics Committee, 'Statement on Medical Age Assessment of Unaccompanied Minor Refugees' 1–6; Pieter JJ Sauer and others, 'Age Determination in Asylum Seekers: Physicians Should Not Be Implicated' (2016) 175 European Journal of Pediatrics 299; A Aynsley-Green and others, 'Medical, Statistical, Ethical and Human Rights Considerations in the Assessment of Age in Children and Young People Subject to Immigration Control' (2012) 102 British Medical Bulletin 17.

authorities.[1441] When she applied for international protection in the Netherlands, she informed the immigration authorities (*Immigratie- en Naturalisatiedienst*, *IND*) that she was fifteen. The IND, however, refused to treat her as a minor, relying upon the data submitted by the Italian counterparts on the basis of the principle of mutual trust. As a result, the minor did not receive appropriate protection, even though she corroborated her statement about her age with documents, and her appearance and behaviour made clear she was a minor at the time. In its decision of April 4, 2019,[1442] the Dutch Council of State (*Raad van State*) affirmed the importance of interstate trust, holding that the State Secretary had – in principle – rightly assumed that the registration of the applicant as an adult had been carried out carefully, so that it was up to the foreign national to demonstrate that the date of birth registered in Italy was incorrect.[1443] In the Court's view, the applicant had failed to do so; a baptism document that was submitted was not accepted, as it was not an identifying document issued by the Eritrean authorities. Furthermore, as a copy of a school card did not include her place of birth, that was also considered insufficient.[1444] Therefore, the Court found that it was correct not to doubt the date of birth registered in Italy and thus to not offer an age test.[1445]

In another case, also from the Netherlands, a data subject asked for international protection in the Netherlands and claimed to be a minor. Subsequently, a search in the Eurodac system revealed that the asylum seeker had previously applied for international protection in Italy, Germany, France, and Switzerland. Investigations in these countries revealed that the asylum seeker was registered there with different dates of birth and aliases. This involved five different registrations as an adult (in Italy, France, Germany, and Switzerland) and one registration as a minor (in Italy). The Secretary of State set the date of birth registered in Switzerland as 1st of January 2002 and considered the foreigner to be of legal age. He therefore did not exam-

1441 This case was found by and first discussed in: Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 410; Raad van State, 11 april 2019, 201803537/1/V1 (*ABR/S*).

1442 201803537/1/V1 *(ABR/S)* (n 1385).

1443 ibid, para 6.

1444 ibid, para 6.1.

1445 ibid, paras 6.1 and 7.

ine the asylum application.[1446] The State Secretary determined: if a foreign national is registered in several Member States with different ages, one or more of which is an adult, the foreign national in question is considered an adult.[1447] The prerequisite is that it can be proven that the respective registration as an adult was carried out carefully. Only if the enquiry does not provide a clear answer and doubts about the age of majority remain, further investigations, such as an age check, should be carried out.[1448] The State Secretary also elucidated: if the Aliens Police and the IND conclude that there is doubt about the age, they will not immediately have an age test carried out; this test is burdensome for a foreign national. In the context of the principle of mutual trust, they may, in principle, assume that the registrations in the other Member States have been carried out carefully.[1449] Enquiries with Switzerland revealed that Switzerland had taken note of the supplementary judgment (*jugement supplétif*) and the extract from the birth certificate. They had changed the date of birth given by the foreign national from 28th of December 2005 to 1st of January 2002 in response to his statements in a brief interrogation.[1450] Since the applicant did not provide any evidence to counter this assessment, this was enough for the Dutch State Secretary to conclude that there were no doubts about the age of the applicant; it set the date of birth, as said, for 1st of January 2002.[1451]

These two cases from the Netherlands show a practice that, in cases of doubt, assumes that young people are of legal age without having carried

1446 Raad van State, 1 november 2022, 202104145/1/V1 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Middelburg, van 23 juni 2021 in zaak nr NL216802*).

1447 ibid, para 3.

1448 ibid, para 3.

1449 ibid, para 3.1.

1450 ibid, para 5.

1451 It is worth mentioning than age assessment cases also exist on the international level. E.g., On the 21st May 2024, the UN Committee on the Rights of the Child (CRC) adopted its decision concerning the communication n°80/2019 (CRC/C/96/D/80/2019). In that case Swiss authorities disregarded the conclusion of an age assessment carried out in Sweden. The CRC concluded that in the absence of a full assessment of the applicants physical and psychological development and of the appointment of a representative to accompany him during the asylum procedure, the best interests of the child had not been a primary consideration, in violation of articles 3 and 12 of the Convention (UN Committee on the Rights of the Child, 'Constatations adoptées par le Comité au Titre du Protocole facultatif à la Convention relative aux droits de l'enfant Établissant une Procédure de Présentation de communications, concernant la communication No 80/2019' (2024) CRC/C/96/D/80/2019).

out an age test. However, there are other cases concerning the determination of the age of adolescents, two of which are presented here. Interestingly, although these cases involve young refugees, they do not relate to the determination of the Member State responsible for the asylum case. Instead, one case concerns whether a guardian should be appointed for the data subject, while the second addresses whether a placement in care should be terminated. Whether the authorities are more inclined to accept that a young person is a minor, if this does not forfeit the possibility of returning this person to another country, cannot be clarified in the context of this study.[1452] In practice, Eurodac entries are created at an early stage, often before the accuracy of the stored data has been fully verified. In Dublin cases, the later application of the principle of mutual trust can further impede more detailed verification.

In the first case, the district court of Geinhausen (*Amtsgericht*) had to decide on the age of a Somali asylum seeker whose asylum case was processed by Germany.[1453] The court reasoned that in order to determine whether a person is a minor, it must determine the facts relevant to the decision ex officio and exhaust all available options for determining age. If no clear determination is possible after these investigations, the court may assume, in favour of the person concerned, that the person is a minor. In the present case, the Hamburg-Eppendorf University Clinic prepared an odontological X-ray diagnostic report to determine the age of the asylum seekers, which concluded with "a probability bordering on certainty" that the asylum seeker was over 18 years old. However, the accuracy of the report was called into question by a birth certificate issued by the Somali embassy, which stated that the data subject in question was under 18. In addition, the data subject argued that the diagnostic report could not be considered reliable due to a lack of comparative material for young people from East Africa. The court concluded that it had exhausted all available

1452 Such an assumption is refuted by other cases, such as Verwaltungsgericht Gera, 27. Oktober 2020, 4 K 203/20Ge, for example, where a supposedly minor asylum seeker was initially sent back from Germany to Italy, but Germany ultimately agreed to carry out the asylum procedure and a precise age assessment was ordered, after the asylum authorities concerned assumed the data subjects was of legal age, without proper procedure. Also, if another Member State registers a data subject as a minor and he or she then travels on, the second State is responsible for the asylum application and cannot send the person back, cf e.g., Landgericht Ingolstadt, 10. Mai 2019, 22 T 742/18, although in this case an age determination was nevertheless ordered.

1453 Amtsgericht Gelnhausen, 12. September 2013, 63 F 641/13 SO.

options for determining age and ultimately assumed that the data subject was a minor.[1454]

What is interesting about this decision is that the court assumes that all possibilities for determining age must be exhausted. This was not assumed in the cases above. Especially when it comes to mutual trust, it seems – according to the Dutch cases – sufficient that another Member State has assumed that a person is of legal age without the need for a thorough investigation.

In the second case, a data subject from Nigeria stated that he was born in 1998.[1455] His passport, the original being available to the immigration authorities, and a visa from the German Consulate General in this passport stated that the person was born in 1994. Accordingly, a placement in care was lifted, which the applicant contested. The Higher Administrative Court of Berlin-Brandenburg (*Oberverwaltungsgericht*) subsequently ruled that, following the summary examination required in the present proceedings, there were considerable doubts as to whether the passport and visa held by the immigration authorities showed the applicant's correct date of birth. The Court opined that there is no document security in Nigeria. Also, the Court held that the visa is only a public document with regard to the content of the decision taken, not the facts on which it is based. Neither the passport nor the visa would therefore provide proof of the accuracy of the date of birth stated therein. The submission of the data subject that he was a minor could therefore not be considered implausible. The Court ruled that an age determination test by an expert should be carried out.[1456]

What is interesting about this case is that the statement of the data subject concerned is regarded as evidence that contradicts the official Nigerian documents. Moreover, the unreliability of the documents is not interpreted to the disadvantage of the young person. Finally, the requirement to exhaust means to clarify the age is also implemented by ordering an age determination test.

As mentioned above, there are many other cases involving the determination or rectification of the age of presumed minors. As already men-

1454 ibid; similarly, in another case, the same diagnostics from the same clinic (but for which the data subject's consent was lacking), together with observations from a personal interview with the data subject, were not sufficient proof that the asylum seeker was of legal age (Oberverwaltungsgericht Bremen, 4. Juni 2018, 1 B 82/18).

1455 Oberverwaltungsgericht Berlin-Brandenburg, 3. April 2013, 6 S 313 and 6 M 513.

1456 ibid; for a similar case also with regard to a data subject carrying a Cameroonian passport see Oberverwaltungsgericht Bremen, 19. Dezember 2018, 1 B 234/18.

tioned, mutual trust can, but should not be, an obstacle to a data subject being able to be heard in a rectification claim. The Eurodac Regulation states that a request for rectification that concerns another Member State must be forwarded to the competent Member State.[1457] Whether this Member State then exhausts all means to determine the age of a person and how it analyses the results of such investigations is still determined by the practice of the respective state.

The Rectifying Place of Entry into the EU or a Category 1 or 2 Hit

Another category of case law occurring frequently are cases where the data subject claims that they have not applied for asylum in a Member State, although Eurodac produces a Category 1 hit (applicants for international protection) instead of or including a Category 2 hit (third-country nationals or stateless persons, apprehended when irregularly crossing the external borders), indicating that they have applied for asylum. A variant of this category are cases where asylum seekers say they have not been travelling through a Member State, although a hit was produced with a data set, stemming from that Member State.

In one instance, the Schleswig-Holstein Administrative Court (*Verwaltungsgericht*) considered a case involving a Eurodac hit of Categories 1 and 2 originating from Hungary. The asylum seeker said that he had not applied for asylum there. The Court opined that, contrary to the asylum seeker's claim, he did indeed apply for asylum. It continued that in cases such as the present one, in which the Eurodac hit and the probable sequence of events were not substantially called into question by the applicant's submission, the court did not consider itself obliged to carry out investigations "into the blue",[1458] i.e., at random.

It is, in principle, correct that submissions to the court must be substantiated. However, the inquisitorial principle (*Untersuchungsgrundsatz*) applies

1457 Eurodac Regulation 2024, Art 43(3).

1458 Verwaltungsgericht Schleswig-Holstein, 27. Juli 2017, 13 A 299/17; similar decisions were also taken in Trier and Madgeburg: Verwaltungsgericht Trier, 18. Oktober 2013, 2 L 1483/13TR; Verwaltungsgericht Magdeburg, 4. März 2014, 9 B 58/14 MD.

in German[1459] (and European[1460]) administrative law: in administrative law proceedings, the court is obliged to investigate the facts of the case *ex officio*. The authority may furthermore not refuse to accept declarations or applications that fall within its remit because it considers the declaration or application to be inadmissible or unfounded.[1461] Moreover, in a case such as the one described above, it is difficult to provide detailed substantiation for a rectification request or to present evidence supporting the claim. Apart from testimonies from the persons involved, no other evidence exists. Of these persons, typically only the asylum seeker's perspective can be heard,

1459 Administrative Procedures Act [1976] (APA - Germany) (VwVfG), § 24 - Untersuchungsgrundsatz; cf Winfried Huck and Martin Müller, '§ 24 - Untersuchungsgrundsatz', *Verwaltungsverfahrensgesetz - Beck'sche Kompakt-Kommentare* (2nd edn, CH Beck 2016); cf also Thorsten Siegel, *Allgemeines Verwaltungsrecht - Lehrbuch & Entscheidungen* (15th edn, CF Müller 2024).

1460 Already in its early case law, the CJEU developed general constitutional principles of administrative procedure under the heading of "principles of sound administration" or "principles of good administration", which include the inquisitorial principle (Matthias Ruffert, 'Artikel 41 GRCh - Recht auf eine gute Verwaltung' in Christian Calliess (ed), *EUV/AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta* (6th edn, CH Beck 2022), para 3, and Rudolf Streinz, 'Artikel 41 GRCh - Recht auf eine gute Verwaltung', *EUV/AEUV: Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrechte der Europäischen Union* (3rd edn, CH Beck 2018), para 5, both with references).

1461 VwVfG, § 24 Untersuchungsgrundsatz states that: "(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden. Setzt die Behörde automatische Einrichtungen zum Erlass von Verwaltungsakten ein, muss sie für den Einzelfall bedeutsame tatsächliche Angaben des Beteiligten berücksichtigen, die im automatischen Verfahren nicht ermittelt würden. (2) Die Behörde hat alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen. (3) Die Behörde darf die Entgegennahme von Erklärungen oder Anträgen, die in ihren Zuständigkeitsbereich fallen, nicht deshalb verweigern, weil sie die Erklärung oder den Antrag in der Sache für unzulässig oder unbegründet hält". ((1) The authority shall investigate the facts of the case *ex officio*. It shall determine the nature and scope of the investigations; it shall not be bound by the submissions and requests for evidence made by the parties involved. If the authority uses automatic devices to issue administrative acts, it must take into account factual information from the party involved which is relevant to the individual case and which would not be determined in the automatic procedure. (2) The authority shall take into account all circumstances relevant to the individual case, including those favourable to the parties involved. (3) The authority may not refuse to accept declarations or applications that fall within its remit on the grounds that it considers the declaration or application to be inadmissible or unfounded on the merits).

while the relevant authorities (e.g., Hungarian authorities, if they could be identified) would not be consulted. Consequently, the evidentiary threshold for demonstrating that the data are incorrect must not be set too high.

In another case from Munich, the Administrative Court also had to judge a Category 1 hit, this time from Italy: the minor asylum seeker stated that he had not applied for asylum in Italy. The Administrative Court of Munich (*Verwaltungsgericht*) opined that if corresponding data are stored in a database such as Eurodac, it can generally be assumed that these data are correct. This applies only in cases where there are no serious doubts about the accuracy of the entry, unless a substantiated submission raises such doubts or a request for rectification has already been submitted. The claimant's assertion alone that he has not submitted an asylum application in Italy does not fulfil these requirements. This applies all the more, the Court held, as it considers it unlikely that the Republic of Italy – knowing full well that a corresponding entry leads to responsibility for an asylum procedure – would register a third-country national as an asylum applicant in Italy in Eurodac if this were not the case.[1462]

Two things are remarkable in this case. Firstly, it is assumed that asylum seekers are a burden for the Member States and that they generally prefer not to register asylum applications. This provides an insight into how asylum seekers are currently perceived in Europe – and might even give an indication of how their value and dignity is assessed. Secondly, it is interesting to note that the court would apparently have heard the argument of the false Eurodac entry in the case of a separate request for rectification. This was probably stated on the assumption that such an application would be substantiated. For the data subject, it may be worthwhile to file an application for rectification immediately upon receipt of a transfer decision in order to suspend the proceedings, so that the argument of the incorrect Eurodac hit at least has to be heard.

The highest German Court (*Bundesgerichtshof*) confirmed that authorities can, in principle, rely on Eurodac data. The Court held, in a case concerning an asylum seeker first registered in Spain, that under the Eurodac Regulation, Member States are required to update data in Eurodac. Specifically, they must record the negative outcome of an asylum procedure. This means that the authorities involved can, in principle, rely on the accuracy

1462 Verwaltungsgericht München, 7. März 2008, M 4 K 0850006.

and completeness of the data in Eurodac and, in particular, trust that an asylum procedure designated as open has not yet been concluded.[1463]

Other Member States follow the same line of argument. According to the Netherlands Council of State (*Raad van State*), the Secretary of State may rely on the information in Eurodac when establishing which Member State is responsible for handling the asylum request.[1464] It is up to the asylum seeker to demonstrate that the registration is incorrect. The Council of State even determined that, only in addition to a Eurodac match or a prior application, other information – such as an original visa issued by another Member State or statements from the asylum seeker about family members or their travel route – may justify a Dublin claim.[1465]

The Swiss Federal Administrative Court (*Bundesverwaltungsgericht*) considered the claims of two asylum seekers who argued that, despite a Eurodac Category 1 hit from Croatia, they had not applied for asylum there. The Court held that it would assume the asylum seekers had, in fact, sought asylum in Croatia. Their contrary claims were deemed insufficient to rebut this presumption, particularly since they acknowledged being apprehended by the Croatian police, who had forcibly taken their fingerprints. The Court noted that the competent Croatian authorities had explicitly consented to the State Secretariat for Migration's readmission request within the prescribed time frame. The authorities indicated that the appellants had expressed an intention to apply for international protection but had absconded before the scheduled interview. Additionally, the Court emphasized that the Dublin III Regulation does not confer on asylum seekers the right to choose the Member State responsible for examining their application.[1466]
It is noteworthy that the coercive circumstances under which the fingerprints were taken had no bearing on the Court's assessment. The judgment also illustrates, in a rather stark way, how the principle of mutual trust operates in practice: as determined by the ECJ in the case above, once a

1463 Deutscher Bundesgerichtshof, 11. Januar 2018, V ZB 28/17.

1464 Raad van State, 1 september 2016, 201604335/1/V3 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 7 juni 2016*); Raad van State, 16 september 2015, 201410018/1/V3 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Groningen, van 20 november 2014).*

1465 201604335/1/V3 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 7 juni 2016*) (n 1464); 201410018/1/V3 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Groningen, van 20 november 2014)* (n 1464).

1466 Schweizerisches Bundesverwaltungsgericht (BVGer), F-12/2023, Urteil vom 27. März 2023, para 5.1, with reference to Tribunal administratif fédéral suisse (TAF) E-5644/2009, Arrêt du 31 août 2010, para 8.3.

Member State agrees to take back an asylum seeker, mutual trust (in principle) precludes an asylum seeker from bringing a claim for rectification. In addition, the 'first state of entry' principle under the Dublin Regulations means that asylum seekers can be sent back to a country in which they have not applied for asylum anyway – whether a (correct) Eurodac entry exists or not.

There are some examples of cases where Eurodac hits were called into question by judges, without the data subjects having to bring forward compelling evidence to this regard. In a case concerning the transfer of an asylum seeker to Italy, the Administrative Court of Cologne (*Verwaltungsgericht*) stated that a Eurodac hit, showing the applicant was apprehended in the town of X in Italy, does not necessarily mean that the asylum application submitted in Germany is a second, and thus ineffective, application. The Court did not clarify if the Eurodac hit was indeed a Category 1 hit, which would imply that an asylum application was submitted in Italy. The Administrative Court then pointed out that there are indications that Italy's procedural practice does not comply with EU or international law standards. The Court supported a temporary injunction, preventing a transfer of the data subject to Italy, but based this on the procedural and accommodation deficiencies in Italy for asylum seekers, not the doubts raised regarding the Category 1 hit.

Similarly, the Administrative Court in Stade, Germany, had to decide in a case in which a removal order from Germany to Greece was contested. There were a Category 1 and a Category 2 hit for Greece in the files.[1467] Yet, the Court found that it cannot be concluded from these Eurodac hits that the data subject has been granted international protection in Greece. The granting of international protection could not be concluded from the applicant's statements, either. He had stated that he had applied for and had been granted asylum in Greece. However, the Court held that it is unclear what the data subject meant by 'asylum'. The application of the claimant provided that, although he was registered in Greece, he was not recognised as a person entitled to asylum. The status of the proceedings was unknown to him. The Court concluded that the removal order was unlawful.

From these cases, it appears that, at least when individuals are being returned to a country where a European court has found deficiencies in asylum procedures or accommodations that violate Art. 4 CFR or Art. 3

1467 Verwaltungsgericht Stade, 7. Oktober 2016, 10 B 2404/16.

ECHR,[1468] evidence beyond Eurodac hits may be considered. There are, however, credible reports and national case law concerning other Member States for which no European-level ruling exists (so far), indicating that irregularities occur in asylum procedures and in the registration of asylum seekers.[1469] Therefore, arguments and evidence that speak against the correctness of Eurodac data should always be heard.

Finally, in a Dutch case, the judge brought forward a legal argument that underlines what some of the judges in the cases above implied but did not seek to justify in law. The case dealt with a Ghanaian national who disputed a Eurodac hit, which suggested that he had provided fingerprints

1468 Regarding Italy, see *Tarakhel v Switzerland* App no 29217/12 (ECtHR, 4 November 2014); Regarding Greece see *M.S.S v Belgium and Greece* App no 30696/09 (ECtHR, 21 January 2011); In its judgment, Case C-808/18 *European Commission v Hungary* [2020], the Court ruled on a breach of EU law by Hungary in the area of, in particular, procedures for granting international protection and procedures for the return of illegally staying third-country nationals. Because Hungary did not implement the Courts judgment, in 2024, the ECJ ruled again and imposed financial sanctions on Hungary, in Case C-123/22 *European Commission v Hungary* [2024] (ECJ, 13 June 2024). These judgments came after the case cited above, in which a deportation to Hungary was carried out without further ado due to a (contested) Eurodac hit.

1469 See e.g. regarding Croatia, the Belgium Council of Alien Law Litigation in its two decisions, Conseil du Contentieux des Étrangers (Belgium Council of Alien Law Litigation), Arrêt n° 278 106 du 29 septembre 2022, dans l'affaire X / III and Conseil du Contentieux des Étrangers (Belgium Council of Alien Law Litigation), Arrêt n° 278 108 du 29 septembre 2022, dans l'affaire X/III, suspended Dublin transfers to Croatia due to structural deficiencies identified for what concerned the asylum procedure and reception conditions, namely, absence of legal aid for part of the procedure and absence of a screening process for torture victims. On 13 April 2022, the Dutch Administrative Jurisdiction Division of the Council of State ruled that the Dutch Immigration and Naturalisation Service (IND) is obliged to do further research on the situation of applicants for international protection being transferred to Croatia under the Dublin III Regulation. This is due to reports of frequent pushbacks (including of applicants who are transferred to Croatia from another EU Member State), which may result in a violation of the principle of non-refoulement. On 30 May 2022, the Minister for Migration announced that until this research is concluded, no Dublin transfers to Croatia will be carried out (European Migration Network, 'EMN Quarterly - Period: April - June 2022' (2022) ed. N.39). Cf also the cases in Germany and Switzerland: Verwaltungsgericht Stuttgart, 2. September 2022, A 16 K 3603/22 and BVGer F-5675/2021, Urteil vom 6. Januar 2022; cf also Lana Tučkorić, 'Country Report: Croatia' (ECRE 2023).

in Switzerland and Italy.[1470] The applicant claimed that he had never been to these countries but travelled through France. The Court decided that the data subject had the right to submit counter-evidence, i.e., that the result of the hit was contestable. The decision was based on a close reading of Art. 22(3) Dublin III Regulation in connection with Annex II, List A of the Commissions Implementing Regulation 118/2014, according to which a "take-charge" request is supported by proof or circumstantial evidence. Proof, which includes a Eurodac hit, is relevant "as long as it is not refuted by proof to the contrary."[1471]

The often blind reliance on Eurodac data confirmed by many Member States, as seen above, is dangerous, especially because there are countries or regions that systemically register asylum seekers incorrectly. In December 2017, a specific procedure was implemented in Questure of Friuli-Venezia Giulia region, on the basis that most of the asylum seekers arriving in this region from Nordic countries or the Balkan route fall under the Dublin III Regulation. The Associazione per gli studi giuridici sull'immigrazione (ASGI) has witnessed cases where the Questure fingerprinted persons seeking asylum in the region as persons in "irregular stay" (Category 3) in the Eurodac database, instead of "applicants for international protection" (Category 1). The Dublin Unit thus justified the implementation of the Dublin transfer prior to the lodging of the application, on the basis that no asylum application has been made.[1472] It is quite possible that this happens in the same way in other Member States, which is why the statements and claims of asylum seekers should be taken seriously – even if, as is often the case, they cannot provide detailed proof.

1470 This case was found by and first discussed in: Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564); Rechtbank Den Haag, 10 december 2019, NL19.24439 *(verzoeker, geboren 2000, van Ghanese nationaliteit / de staatssecretaris van Justitie en Veiligheid)*.

1471 Under the AMMR, Art 40 regulates take-charge requests, stating in para. 4: "The Commission shall, by means of implementing acts, establish, and review periodically, two lists, indicating the relevant elements of proof and circumstantial evidence in accordance with the criteria set out in the second and third subparagraphs of this paragraph. Those implementing acts shall be adopted in accordance with the examination procedure referred to in ibid, Art 77(2)." The Implementing Acts have not yet been issued.

1472 Caterina Bove, Matteo Astuti and Chiara Pigato, 'Country Report: Italy' (ECRE 2023) 74.

Evidential Value of Eurodac Data

The question of the evidential value of Eurodac data and the standard of proof applied when an applicant or a Member State claims that the data are incorrect has been addressed in two older UK cases from 2007. These cases provide interesting insights into how a Eurodac hit can be understood from an evidentiary perspective.[1473] What was decided with regard to the standard of proof in these cases will be discussed in the next chapter on the right to an effective remedy. However, one statement of the court in one of these cases shall be mentioned here: it shows that Eurodac data, for a long time, not only have been used as evidence to determine which Member State is responsible for the processing of an asylum application but also beyond that. The Asylum and Immigration Tribunal held that "[w]e are satisfied that fingerprint evidence from the Eurodac system is admissible in evidence not only when considering which member state is responsible for examining the application for asylum but also generally as part of the examination of the claim."[1474] The Tribunal continued that lawful use of the Eurodac data does not come to an end with the identification of the Member State responsible for processing the asylum claim.[1475]

This early use of Eurodac data as evidence used beyond their function in connection with the Dublin Regulation has been massively expanded to date. In the meantime, as this study shows, Eurodac data are used for very different and particularly security-related purposes. It is also used as evidence accordingly. Its evidential value has increased. Nonetheless, the question arises whether, with the increasingly widespread use of Eurodac data, it can still be confidently relied upon, as discussed above.

Considering that Eurodac data can be used as evidence within the examination of an asylum claim, this next case is of interest, although it does not directly concern Eurodac data. The High Court of Ireland decided that the International Protection Appeals Tribunal & Anor had erred in law by proceeding under the premise that evidence in an asylum procedure could not be considered until general credibility was acknowledged.[1476] The High Court upheld the appeal of an asylum seeker from Pakistan who had sought international protection in Ireland but was rejected and sent

1473 YI, *Eritrea v Secretary of State of Home Department* (n 1198).

1474 RZ, (Eurodac - Fingerprint Match - Admissible) *Eritrea v Secretary of State for the Home Department* [2008] AIT 00007, para 42.

1475 ibid, para 43.

1476 High Court of Ireland, IEHC 372 High Court Judical Review: *M.H. v the International Protectional Appeals Tribunal* [2023] No. 2022/669 JR 3.

the case to a different Tribunal member for a new review. It determined that the findings were made without considering any potential supporting documentation provided by the applicant, because he was not deemed credible in the first place. Although general credibility is a consideration when evaluating submitted documents and may be decisive, the Tribunal erred in law by proceeding on the premise that documents could not be accepted unless general credibility was established, failing to recognise that there is a requirement to evaluate documents as to their contents in addition to general credibility.[1477]

Another case that provides some insight into the evidentiary value of Eurodac data stems from the Netherlands. This case concerned the admissibility of an asylum application by a data subject who presumably held a residence permit in Greece and the extent to which the State Secretary ought to further investigate the validity of that permit.[1478]

The Dutch Council of State (*Raad van State*) ruled on the declaration of an asylum application as inadmissible by the State Secretary and corresponding refusal to grant a temporary residence permit.[1479] It did so because the data subject in question presumably already enjoyed international protection in Greece, as per the corresponding Eurodac record dated from a year and a half earlier. Records by beneficiaries of international protection are marked in Eurodac (then, according to Art. 18(1) Eurodac Regulation 603/2013, under the new Eurodac Regulation according to Art. 31(2)). Under the previous Eurodac system, marked data were blocked after three years. As a result, it would return a negative outcome to the requesting Member State in the event of a hit.[1480] Under the new law, data are made available for comparison for law enforcement purposes, until such data are automatically erased pursuant to Art. 29(1) Eurodac Regulation, i.e., after a decade. If the status of a data subject is revoked, who previously enjoyed, as in this case, international protection, the Member State has to unmark or unblock the data.[1481] Art. 18(3) Eurodac Regulation 603/2013 (and now,

1477 ibid.

1478 This case was found by and first discussed in: Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564); 201604335/1/V3 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 7 juni 2016*) (n 1464).

1479 201604335/1/V3 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 7 juni 2016*) (n 1464).

1480 Eurodac Regulation 603/2013, Art 18(2).

1481 ibid, Art 18(3); Eurodac Regulation 2024, Art 31(3).

Art. 31(3) Eurodac Regulation) does not prescribe specific time limits for national authorities to update the relevant records. The Council of State confirmed that the State Secretary may, in principle, rely on information from another Member State; it only has a duty to verify the information under certain circumstances.[1482] The Council of State ruled that it could not be assumed that the information was updated and had to be further investigated.[1483] The right to rectification was thus granted in this case: the information's accuracy could not be readily assumed in the absence of a time limit.

What distinguishes this case from some of the above is that the absence of a time limit can be considered to be a legal uncertainty, while age or travelling routes cannot. The latter are, however, factual uncertainties, which, it is argued here, should also be considered within the right to rectification.

Justiciability

As explained above, one has to ask what grounds can be put forward for the rectification of data and whether, for example, a breach of security provisions is considered as such. As mentioned, security standards regarding fingerprint matching have been lowered, as Art. 38(4) Eurodac Regulation only provides for a fingerprint expert "where necessary" other than under Art. 25(4) Eurodac Regulation 603/2013. The obligation to have a fingerprint expert verify the results of a match, as was stated in Art. 25(4) Eurodac Regulation 603/2013, was not justiciable – at least in France – unless where the reliability of the information resulting from the comparison was seriously criticised.[1484]

This case is particularly interesting because, in connection with Eurodac data, the question as to what happens if certain security standards are not met will certainly arise again. For example, what if it emerges that in certain countries or by certain authorities (more or less systematically), the procedures for access to data for (law enforcement) authorities have not been followed – or officials without access authorisation have been given access by other authorised officials? What if certain security precautions for data storage are not observed? What if the data quality in certain countries cannot be guaranteed, because the asylum procedures lead to too many

1482 cf Raad van State, 12 augustus 2014, 201304293/1/V4 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Arnhem, van 18 april 2013)*.

1483 201604335/1/V3 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 7 juni 2016*) (n 1464).

1484 CAA de Lyon, 18LY01453 (n 855), para 8.

errors when more biographical data and more biometric data will be stored etc.? In the aforementioned French case, the court does not seem to have investigated whether the security provision in Art. 25(4) Eurodac Regulation 603/2013 was systematically violated. Additionally, it appears that the data subject did not request this investigation, nor was there any inquiry into whether a fingerprint expert was regularly consulted. In future similar cases, a data subject may want to bring such a question before the national data protection authority. Even if there were systemic flaws in Eurodac registration or processing operations, similar to those in the asylum procedure, would this render Eurodac data unreliable as proof or circumstantial evidence? Would the Member State then be required to provide additional evidence to verify the accuracy of the Eurodac data? Furthermore, would it need to delete the data if security gaps are discovered? This study argues that, at least in the case of systematic irregularities regarding Eurodac data, as observed above in the Questure of Friuli-Venezia Giulia region, the principle of mutual trust does not apply and Eurodac data cannot be considered as full proof.

Human Mistakes and Manipulation

What should always be borne in mind in this context is that errors relating to Eurodac data can sometimes occur not within the Eurodac system, but outside it. Often, it will be humans who make mistakes, not a technical system. This is the case when authorities register incorrect or incomplete data in Eurodac, as some cases above already demonstrated. It can also be illustrated by a case from Germany. In a case from a Regional Court in Landshut (*Landgericht*), the data subject concerned had applied for asylum in Italy before they applied, again, in Germany. This was, according to the Court, evident from the Eurodac match obtained at the time of the arrest of the data subject in Germany. However, the Eurodac hit was then not taken on file due to an error at the Federal Police (*Bundespolizei*). This resulted in the Federal Police attempting to deport the person to Pakistan for weeks, instead of transferring him to Italy by way of the Dublin procedure. The Regional Court pointed out that the error by the Federal Police constituted a breach of the principle of acceleration and that the deportation order was unlawful. The Regional Court deemed it irrelevant that the data subject initially concealed his asylum application in Italy, noting that it is not uncommon for authorities to receive false information

from asylum applicants.[1485]
In this case, a request for rectification of the Eurodac data would not have led to the desired result because the data were correct but were not filed and used correctly later.

On the other hand, asylum seekers that deliberately provide incorrect data to Eurodac can be severely penalised. In Germany, the Federal Administrative Court (*Bundesverwaltungsgericht*) has ruled that an asylum application does not have to be processed if a data subject deliberately conceals or attempts to manipulate data stored in Eurodac. This was decided in a case relating to the manipulation of fingerprints.[1486] The German Federal Administrative Court writes that the asylum seeker is not obliged to guarantee that the fingerprints they provide can be analysed in the Eurodac system because of the obligation to tolerate these identification measures. They are still obliged to refrain from all measures that make it difficult or impossible to establish their identity on the basis of the statutory provisions.[1487] In cases where there are indications that the fingertips have been manipulated, there exists a suspicion that the asylum seeker has thwarted the usability of their fingerprints through their own actions in order to conceal their true identity. Such conduct is liable to call into question the genuineness of the asylum application. In consequence, a legal fiction applies whereby the application is treated as having been withdrawn.[1488] In this context, the question arises as to the circumstances in which a

1485 Landgericht Landshut und Amtsgericht Erding, 7. Oktober 2016, 64 T 853/18 & 6 XIV 41/18 (B).

1486 Bundesverwaltungsgericht im Namen des Volkes Urteil (BVerwG), 5. September 2013, 10 C 1.13; cf also in France, the decision of the Cour Nationale du Droit d' Asile (Cour Nationale du Droit d'Asile, du 21 février 2012, N° 11032252) in a similar case. In an internal memo the Office for the Protection of Refugees and Stateless Persons (Office Français de Protection des Réfugiés et Apatrides (OFPRA)) Director General instructed the heads of geographical divisions to take standard rejection decisions for asylum seekers because the prefectures were unable to read their fingerprints. More than five hundred applications were rejected without an interview. The note was challenged in front of the National Court of Asylum Rights by a person whose asylum application had been rejected by OFPRA. The Court rules that "the provisions [of the Code de l'entrée et du séjour des étrangers et du droit d'asile] preclude OFPRA, when seized of a duly registered asylum application, from rejecting it without having ruled on the applicant's possible right to protection as an asylum seeker following a specific examination of the elements presented in support of his application." The Court did not, however, decide, what happens if the asylum seeker did indeed manipulate its fingerprints.

1487 BVerwG 10 C 1.13 (n 1486), para 22.

1488 ibid, para 29.

deception as to identity is deemed to have occurred, for example where false statements concerning biographical particulars are provided. The aim of interoperability, or the MID as part of it, is to uncover multiple identities. This is only possible if a person is recorded in several databases that are connected to the interoperability system or is recorded multiple times in one (that stores biometric data). In other cases, this will likely not be detected by the MID, but may lead to problems later on (for example, if another person wants to enter the EU with the same identity). Particularly in the context of individuals seeking international protection, it is essential not to precipitously infer that they are attempting to conceal their identity when inaccurate data are recorded in Eurodac. This consideration will become increasingly significant as the volume of data stored in Eurodac expands. It is anticipated that errors in biographical information will increase, and that technical limitations inherent in facial recognition software will further contribute to such inaccuracies.

4. Conclusions

The Eurodac and Interoperability Regulations aim to provide a structured framework for the rectification, completion, and erasure of data and information as well as the restriction of data processing. Still, several significant limitations and complexities persist.

While Art. 43 of the Eurodac Regulation provides for the rectification or erasure of inaccurate or unlawfully recorded data, it does not explicitly define which categories of data may be subject to these processes. This is particularly concerning in light of the introduction of the security flag. Data subjects designated as security threats should be informed and given the opportunity to challenge this categorisation. However, the Eurodac Regulation does not clearly delineate which aspects of the security flag are subject to rectification or erasure, and it expressly permits restrictions on these rights. In the absence of precise guidance, national practices may diverge, thereby potentially undermining the effectiveness of access to justice.
The verification process for fingerprint matches under the new Eurodac Regulation is discretionary, potentially reducing the reporting and correction of false hits, which could mislead the perceived accuracy of Eurodac technology.
Furthermore, there is a lack of robust mechanisms to ensure that rectifications are communicated to previous recipients of data, such as law enforce-

ment authorities or third countries. There is also considerable ambiguity regarding when entities that have extracted or received data from Eurodac are obliged to erase them. This uncertainty extends to ongoing investigations, which permit authorities to retain data for longer periods.

With regard to the Interoperability Regulation, Art. 48 offers only limited possibilities for rectifying or erasing data, as it applies solely to the MID. Errors in the MID often necessitate rectification of corresponding data in the CIR and sBMS. However, correcting data in the CIR or sBMS requires either a GDPR-based request or a direct appeal to the underlying database, such as Eurodac. This fragmented framework complicates and delays rectifications, thereby undermining both effective access to justice and overall efficiency.

The Interoperability Regulations do not provide data subjects with access to logs of data processing operations, making it difficult to identify the authorities responsible. To mitigate this and strengthen accountability, a mandatory obligation to notify all authorities that have accessed the data in cases of rectification or erasure would be advisable. Furthermore, the introduction of white and red links in the MID may inadvertently prolong data retention periods in the CIR, creating potential conflicts with legal time limits. Finally, it has been observed that although automated data quality control mechanisms generate alerts when data fail to meet required standards, it remains unclear to what extent these alerts are accessible to authorities or data subjects.

These questions and issues arise directly from the texts of the Eurodac and Interoperability Regulations themselves. At the same time, practical implementation adds challenges. As this study has shown, requests for rectification, completion, and erasure can be submitted in any Member State. This may benefit individuals, as they can file requests in a familiar language and seek assistance from trusted persons, lawyers, or specialised organisations. However, requirements to provide detailed reasons for a request may add significant complexity. Data subjects may be expected to clearly identify inaccuracies and substantiate their claims with justifications or evidence. While such requirements are appropriate in formal legal proceedings, they can pose major hurdles in data-related cases – particularly for individuals without specialised legal representation. Where automated processing is involved – such as fingerprint matches or MID links – it is difficult for data subjects to understand the processes and even more difficult to supply supporting evidence. Also, demonstrating the absence of data or the need

for completion is particularly challenging when relevant documentation is missing or not recognised by Member States.

Another aspect addressed in this chapter concerns the challenges that give rise to inaccurate data. Asylum procedures conducted under significant time pressure – such as so-called border procedures – combined with insufficient legal support and/or translation, risk generating false or incomplete records. The consequences of such inaccuracies may be amplified by interoperability mechanisms: erroneous data that are exchanged and subsequently processed across multiple systems can create additional complications. In Eurodac, inaccuracies compounded by expanded data storage and interoperability pose substantial risks. The evidentiary weight attributed to Eurodac data frequently outweighs other forms of evidence, thereby creating procedural obstacles to rectification. While courts may place considerable reliance on Eurodac 'hits', they should nonetheless scrutinise them carefully, particularly where systemic issues or procedural irregularities are apparent. The principle of mutual trust enables authorities to presume the accuracy of data originating from other Member States, with the aim of facilitating cross-national procedures and decision-making. Yet this principle does not always assist in the rectification or completion of data entries. At times, it conflicts with the right to be heard and the effective enforcement of the right to rectification. As national case law demonstrates, such tensions can result in questionable outcomes.

Overall, the Eurodac and Interoperability Regulations establish a framework for the rectification, completion, and erasure of data, as well as for the restriction of data processing. However, limitations and ambiguities in the legal text, together with practical challenges, may impede the full realisation and effective implementation of these rights. Therefore, the fragmented nature of data management must be addressed with a view to access to justice, particularly for data subjects – most often asylum seekers – who need to understand where and how their data are stored and how they can request rectification or erasure. Evidentiary challenges in data-related cases have long been recognised and are likely to intensify as technology continues to develop rapidly. These challenges require careful attention.
Moreover, as the broad interpretation of the principle of mutual trust may complicate rectification and erasure processes, this principle needs to be looked at through a lens of the digital developments. Moreover, as the broad interpretation of the principle of mutual trust may complicate rectification and erasure processes, this principle should be carefully examined and adapted in the context of digital developments. Otherwise, while

this principle is justified within the EU, in a data-driven, cross-national system such as the interoperable Eurodac system, it may impede justice and fairness. Addressing these issues is essential to enhance data accuracy, reliability, and fairness, ensuring that data subjects can effectively exercise their rights without undue burden.

IV. The Right to an Effective Remedy

1. What Is the Right to an Effective Remedy?

This chapter examines the remedies provided under the Eurodac and Interoperability Regulations in relation to Eurodac data, and assesses whether these remedies can be considered 'effective'. It begins by outlining the prerequisites for an effective remedy under various human rights regimes, with particular attention to the divergences between the jurisprudence of the CJEU and the ECtHR. It then analyses the remedies specifically provided in the Eurodac and Interoperability Regulations, as well as the remedies available under the AMMR for addressing issues related to Eurodac data. The second part of the chapter considers the scope of these remedies and the practical challenges they entail, addressing procedural questions such as which acts and decisions can be contested, issues arising in composite procedures, and matters concerning mutual trust and the burden of proof. Finally, the chapter examines specific acts and decisions relating to Eurodac data to evaluate whether they can be effectively challenged in practice.

a) *International Human Rights Instruments*

Most global and regional human rights instruments provide a right to a remedy. The UDHR, although not binding, states in Art. 8 that "[e]veryone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law." Other binding legal instruments contain the same right. The ICCRP encompasses a right to an effective remedy in its Art. 2(3), 9(5) and 14(6). The CRC declares "a right to challenge the legality of the deprivation of [a child's] liberty […]" in Art. 37(d), while the general right to a remedy is part of Art. 3 CRC. Regarding persons with disabilities, the Convention on the Rights of Persons with Disabilities (CRPD) demands in Art. 13 "effective access to justice for persons with disabilities on an equal basis with others […]". In view of the wide recognition of this right, it can even be considered a norm of customary international law.[1489]

1489 Dinah Shelton, 'Sources of Article 47 Rights' in Steve Peers, Tamara Hervey and Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (1st edn, Hart Publishing 2014).

b) *Regional Human Rights Instruments: ECHR and CFR*

aa) ECHR

In the ECHR, the right to an effective remedy is primarily contained in Art. 13. The provision is modelled on Art. 8 UDHR.[1490] Art. 13 ECHR is of great importance in the case law of the ECtHR. It secures the granting of an effective remedy before a national authority to everyone whose Convention rights and freedoms have been violated. Art. 35(1) ECHR reveals that "[t]he Court may only deal with the matter after all domestic remedies have been exhausted." The machinery of complaint to the Court is thus subsidiary to national systems safeguarding human rights.[1491] Art. 35(1), in giving direct expression to the States' obligation to protect human rights first and foremost within their own legal system, establishes an additional guarantee for an individual in order to ensure that they effectively enjoy those rights.[1492] Art. 13 ECHR can only be invoked and exercised in combination with a violation of a substantive provision in the ECHR.[1493] Insofar, Art. 13 merely complements the other substantive clauses of the Convention and its Protocols.[1494]

Contracting States have a margin of appreciation in conforming with their obligations under Art. 13 ECHR.[1495] No particular form of remedy is

1490 ibid.

1491 *Kaemena and Thöneböhn v Germany* App no 45749/06 and no 51115/06 (ECtHR, 22 April 2009), para 77; Council of Europe, *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights: Volume II: Consultative Assembly, Second Session of the Committee of Ministers, Standing Committee of the Assembly (10 August-19 November 1949)* (Brill | Nijhoff 1975) 485 - 490; Council of Europe, *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights: Volume III: Committee of Experts (2 February-10 March 1950)* (Brill | Nijhoff 1976) 651.

1492 *Kudla v Poland* ECHR 2000-XI, para 152; ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827).

1493 Denise Renger, 'Artikel 13 - Recht auf wirksame Beschwerde', in Jens Meyer-Ladewig and Martin Nettesheim (eds), *EMRK Europäische Menschenrechtskonvention, Handkommentar* (5th edn, Nomos 2023), para 1.

1494 *Toplak and Mrak v Slovenia* App no 34591/19 and 42545/19 (ECtHR, 26 October 2021), para 79.

1495 *Vilvarajah and Others v the United Kingdom* (1991) Series A no 215, s 122; *Chahal and Others v United Kingdom* (n 1308), s 145; *Smith and Grady v United Kingdom* ECHR 1999-VI, s 135.

required.[1496] The national authority before which a remedy will be effective may be a judicial or non-judicial body.[1497] It may be a quasi-judicial body (such as an ombudsman),[1498] an administrative authority (e.g., a government minister),[1499] or a political authority (for instance, a parliamentary commission).[1500] The scope of what possibly counts as an effective remedy under Art. 13 ECHR is therefore broader than that of Art. 47 CFR, as will be detailed later. However, the authority's powers and the procedural safeguards that it affords are taken into account in order to determine whether the remedy is effective;[1501] and the authority has to be independent.[1502] Furthermore, a non-judicial body must normally have the power to hand down a legally binding decision.[1503]

Art. 13 ECHR requires that a domestic remedy afford the possibility of dealing with the substance of an "arguable complaint" under the Convention and of granting appropriate relief.[1504] The ECtHR does not give an abstract definition of the notion of arguability. It decides on a case-by-case basis whether a claim was arguable and, if so, whether the requirements of Art. 13 ECHR were met in relation thereto.[1505]

1496 *Budayeva and Others v Russia* App no 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02 (ECtHR, 20 March 2008), s 190.

1497 *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights: Volume II* (n 1491) 485 - 490; *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights: Volume III:* (n 1491) 651.

1498 *Torsten Leander v Sweden* (n 523).

1499 *Boyle and Rice v the United Kingdom* (1988) Series A no 131.

1500 *Klass and Others v Germany* (1978) 2 EHRR 214.

1501 ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 29; *Klass and Others v Germany* (n 1500), s 67; *Silver and Others v United Kingdom* (1983) 5 EHRR 347, para 113; *Kudla v Poland* (n 1492), para 157; *Mugemangango v Belgium* App no 310/15 (ECtHR, 10 July 2020), para 67.

1502 *Torsten Leander v Sweden* (n 523), para 77(b) and 81.

1503 ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 30.

1504 cf *Boyle and Rice v the United Kingdom* (n 1499); *Powell and Rayner v United Kingdom* (1990) 12 EHRR 335; *M.S.S v Belgium and Greece* (n 1468).

1505 ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 13; referring to: *Boyle and Rice v. the United Kingdom* (n 1499), para 55; *Plattform "Ärzte für das Leben" v Austria* (1988) Series A no 139, para 27; *Esposito v Italy* App no 35771/03 (ECtHR, 27 November 2007).

The term 'effective' means the remedy must be sufficient and accessible, fulfilling the obligation of promptness.[1506] The remedy must enable the submission of a complaint about the alleged violation of the Convention.[1507] Excessively restrictive requirements may render the remedy ineffective.[1508] Remedies must be accessible for the person concerned.[1509] The domestic authorities ruling on the case must examine the merits of the Convention complaint.[1510] Thus, the effectiveness of the remedy is assessed in relation to each complaint[1511] and *in concreto*.[1512]

There is some overlap between Art. 13 ECHR and Art. 6(1) ECHR. Art. 6(1) guarantees the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law in civil and criminal matters. Additionally, Art. 5(4) ECHR provides a *habeas corpus* guarantee. The requirements of Art. 6 ECHR may also be relevant for assessing the effectiveness of a remedy under Art. 13 ECHR.[1513] As a general rule, the fundamental criterion of fairness, which encompasses the equality of arms, is a constitutive element of an effective remedy. A remedy cannot be considered effective unless the minimum conditions enabling an applicant to challenge a decision that restricts their rights under the Convention are provided.[1514] Art. 6 and 13 ECHR establish a positive obligation for the parties to the Convention to actively create effective legal protection mechanisms.[1515] In particular, the fundamental right of access to

1506 *Paulino Tomás v Portugal* ECHR 2003-VIII; *Çelik and İmret v Turkey* (2005) App no 44093/98, para 59.

1507 ECHR 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 37.

1508 ibid, no 38.

1509 ibid, no 39; cf also Renger, 'Artikel 13 - Recht auf wirksame Beschwerde' (n 1493), no 9ff.

1510 ECtHR 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 34; with reference to *Smith and Grady v United Kingdom* (n 1495), para 138; *Peck v United Kingdom* ECHR 2003-I, paras 105-106; *Hasan and Chaush v Bulgaria* ECHR 2000-XI, paras 100 ff.

1511 ECtHR 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 34.

1512 *Colozza and Rubinat v Italy* (1982) 28 DR 149, 146 - 147.

1513 ECtHR 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 36.

1514 *Csüllög v Hungary* App no 30042/08 (ECtHR, 7 June 2011), para 46; ECtHR 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), no 36.

1515 Christoph Grabenwarter, 'Article 13 - Right to an Effective Remedy', *European Convention on Human Rights: Commentary* (1st edn, CH Beck - Hart - Nomos

these mechanisms must exist "in concrete terms and not as a theoretical abstraction".[1516]

The ECtHR has, in many cases, defined what an effective remedy must afford with regard to immigration and asylum law.[1517] At its core, the Court demands that, whenever there is a risk of violation of the guarantees in Art. 2 or 3 ECHR, there must be an effective remedy[1518] which guarantees access, quality and promptness.[1519] The effectiveness of a remedy imperatively requires independent and rigorous scrutiny by a national authority of any claim that there exist substantial grounds for fearing a real risk of treatment contrary to Art. 3 ECHR.[1520] National authorities must refrain from asking strict proof of an applicant regarding the risk of an infringement of Art. 2 or 3 ECHR or putting on them the full burden of proof;[1521] remedies must have suspensive effect.[1522] Finally, applicants have to be provided with sufficient information regarding their rights.[1523]

- Helbing Lichtenhahn Verlag 2014), paras 5 and 16; Renger, 'Artikel 13 - Recht auf wirksame Beschwerde' (n 1493), para 9ff; Cançado Trindade Augusto Antônio, *Access of Individuals to International Justice* (Oxford University Press 2011) 60 with references; Timo Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (Mohr Siebeck 2014) 170.

1516 Augusto Antônio, *Access of Individuals to International Justice* (n 1515) 60 with references.

1517 cf Renger, 'Artikel 13 - Recht Auf Wirksame Beschwerde' (n 1493), para 9ff; cf also Grabenwarter, 'Article 13 - Right to an Effective Remedy' (n 1515), para 17.

1518 *Khlaifia and Other v Italy* App no 16483/12 (ECtHR, 15 December 2016), para 276; *Singh and Others v Belgium* App no 33210/11 (ECtHR, 2 October 2012), para 78ff; *G.H.H and Others v Turkey* ECHR 2000-VII, para 36.

1519 *E.H. v France* (n 1418), para 177ff.

1520 cf *M.S.S v Belgium and Greece* (n 1468), para 293, with further references.

1521 *Allanazarova v Russia* App no 46721/15 (ECtHR, 14 February 2017), para 103; *Rustamov v Russia* App no 11209/10 (ECtHR, 3 July 2017), para 117; *M and Others v Bulgaria* (2011) App no 41416/08, para 127.

1522 *E.H. v France* (n 1418), para 177; *S.K. v Russia* App no 52722/15 (ECtHR, 14 February 2017), para 81.

1523 *D v Bulgaria* App no 29447/17 (ECtHR, 20 July 2021), para 116; *Hirsi Jamaa and Others v Italy* App no 27765/09 (ECtHR, 23 February 2012), para 204; regarding the requirement to provide information in a language that the data subject (in this case a minor) can understand: *Rahimi v Greece* App no 8687/09, (ECtHR, 5 April 2011).

bb) CFR

Art. 47(1) CFR provides a right to an effective remedy before a tribunal for everyone whose rights and freedoms under EU law are violated. Art. 47(2) CFR guarantees a right to a fair and public hearing by an independent and impartial tribunal as well as a possibility to be advised, defended, and represented. Art. 47(3) CFR is dedicated to legal aid. The CJEU treats Art. 47(1) as *lex generalis* from which the other Art. 47 CFR rights are derived.[1524]

The right to an effective remedy must be granted to ensure the correct application of both Union measures and Member States' measures, which are intended to give effect to Union law and fall within its scope of application.[1525] In the EU legal order, the right to effective judicial protection has been recognised as applying to the field of administrative law, notably where a deportation order is challenged.[1526] Art. 47 CFR does also not draw a distinction between criminal and administrative law measures, so the same standards apply.[1527]

Art. 47(1) CFR is based on Art. 13 ECHR. This, as stated above, provides that everyone whose rights and freedoms are set forth in the Convention has an effective remedy before a national authority.[1528] However, Art. 47 CFR guarantees the right to an effective remedy before a tribunal. Unlike the protection under the ECHR, a remedy before a non-judicial authority is not sufficient.[1529] The requirement that the effective remedy has to be

1524 Clara Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Publishing 2021), para 47.08, with reference to case law.

1525 Lock and Martin, 'Article 47 CFR' (n 885), para 7; cf CFR, Art 51(1).

1526 Lock and Martin, 'Article 47 CFR', (n 885), para 3; Case 98/79 *Josette Pecastaing v Belgian State* [1980] ECR 691.

1527 Lock and Martin, 'Article 47 CFR', (n 885), para 7; Case C-386/10 P *Chalkor AE Epexergasias Metallon v European Commission* [2011] ECR I-13085, para 50.

1528 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.16.

1529 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 47 - Right to an Effective Remedy and to a Fair Trial; Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.17; Case 222/84 *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* [1986] ECR 1651; *Unectef v Georges Heylens and others* (n 1127); Case C-97/91 *Oleificio Borelli v Commission of the European Communities* [1992] ECR I-6313; Case C-104/91 *Aguirre Borrell and Others* [1992] ECR I-3003.

– ultimately – a judicial one is based on the CJEU's case law.[1530] What constitutes a 'tribunal' is not defined in the provision. The relevant criteria are those the CJEU considers when determining whether a body is a court or tribunal for the purposes of Art. 267 TFEU.[1531] For example, in the Wilson case in 2006, the ECJ found that the principle of effective judicial protection required that there must be actual access to the courts, which must be independent and impartial as well as be competent to rule on both facts and the law.[1532]

Another core element of Art. 47(1) CFR is that remedies for violations of rights and freedoms guaranteed by EU law need to be effective and real.[1533] This implies certain rights of defence. For example, the persons concerned must be able to ascertain the reasons upon which a decision in relation to them is based, so that they are able to defend their rights in the best possible way.[1534]

1530 Lock and Martin, 'Article 47 CFR', (n 885), para 4; Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.17; Case C-682/15 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* [2017] OJ C 239/8, para 52; Joined Cases C-245/19 and C-246/19 *État luxembourgeois v B and État luxembourgeois v B, C, D and F.C.* [2020], Opinion of AG Kokott, para 52–57.

1531 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.09; Case C-17/00 *François De Coster v Collège des bourgmestre et échevins de Watermael-Boitsfort* [2001] ECR I-09445, para 10; Case C-58/13 *Torresi v Consiglio dell'Ordine degli Avvocati di Macerata* [2014] OJ C 315/9, para 17; Case C-64/16 *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* [2018] OJ C 142/2, para 38; Case C-619/18 *European Commission v Republic of Poland* [2019] OJ C 280/9, para 55; on the concept of a court or tribunal and the autonomy of EU law, see Case C-284/16 *Slowakische Republik v Achmea BV* [2018] OJ C 161/7; Opinion 1/17 On the EU-Canada CETA Agreement (n 826).

1532 Case C-506/04 *Graham J Wilson v Ordre des avocats du barreau de Luxembourg* [2006] ECR I-8613, para 48ff; see more recently, e.g., Joined Cases C-585/18 and C-625/18 *AK v Krajowa Rada Sądownictwa and DO v Sąd Najwyższy* [2019] OJ C 27/6, para 165.

1533 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.09; Joined Cases C-133/19, C-136/19 and C-137/19 *B M M and Others v État belge* [2020] OJ C 297/14, para 54; cf also Joined Cases C-133/19, C-136/19 and C-137/19 *B M M and Others v État belge* [2020], Opinion of AG Gerard Hogan, para 44, and his discussion of relevant case law of the European Court of Human Rights.

1534 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.09; cf e.g., *ZZ v Secretary of State for the Home Department*, (n 559) para 53; Case C-348/12 P *Council of the European Union v Manufacturing Support & Procurement Kala Naft Co, Tehran* [2013] OJ C 39/6, para 68; Case C-34/17

Art. 47(2) CFR also corresponds to Art. 6(1) ECHR.[1535] Other than Art. 6(1) ECHR, the right to a fair trial conferred by Art. 47(2) CFR is not restricted to disputes relating to civil rights and obligations and criminal charges. It applies to all proceedings within the scope of EU law, including administrative proceedings.[1536] This is an important difference between Art. 47(2) CFR and Art. 6(1) ECHR. The broader scope of the Charter is a consequence of the fact that the EU is a union based on the rule of law.[1537] Art. 47(2) CFR elaborates upon the right to an effective judicial remedy by stipulating a number of procedural rights aimed at ensuring a fair trial. The first sentence comprises six different elements: a fair trial, a public hearing, an independent tribunal, an impartial tribunal, a tribunal that was previously established by law and, finally, adjudication within a reasonable period. Attached to these elements is, seventh, a right to be advised, defended and represented, which is enshrined in the second sentence of Art. 47(2) CFR.[1538] An essential component of the right to a fair trial is the principle of equality of arms, or procedural equality.[1539] Another essential component of the right to a fair hearing is the right to adversarial proceedings.[1540] The right to a fair hearing essentially includes the right to equality of arms, the right to adversarial proceedings and the right to a reasoned decision, as well as the right to secure the execution of a final judgment.[1541] A public hearing

Eamonn Donnellan v The Revenue Commissioners [2018] OJ C 211/5, para 55; Case C-230/18 *PI v Landespolizeidirektion Tirol* [2019] OJ C 230/15, para 78.

1535 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 47 - Right to an Effective Remedy and to a Fair Trial; "[…] inspired by Article 6 of the ECHR" Joined Cases C-174/98 P and C-189/98 P *Kingdom of the Netherlands and Gerard van der Wal v Commission of the European Communities* [2000] ECR I-00001, para 17.

1536 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 47 - Right to an Effective Remedy and to a Fair Trial. Note that the Explanation refers only to civil rights and obligations and omits criminal charges.

1537 ibid; Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.19.

1538 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.10; Lock and Martin, 'Article 47 CFR' (n 885), para 31.

1539 Lock and Martin, 'Article 47 CFR' (n 885) para 29; with reference to Case C-514/07 *P Sweden and Others v API and Commission* [2010] ECR I-08533; Case C-205/15 *DGRFP v Vasile Toma and Biroul Executorului Judecătoresc Horațiu-Vasile Cruduleci* [2016] OJ C 335/19.

1540 FRA et al, *Handbook on European Law Relating to Access to Justice* (n 204) 40.

1541 ibid.

ensures scrutiny of the judiciary. The right to a public hearing also requires that an individual has the right to attend and hear evidence.[1542]

In addition, Art. 47(3) CFR requires legal aid to be made available to those who lack sufficient resources.[1543] Art. 47(3) CFR derives from the case law of the ECtHR.[1544] The notion of 'legal aid' encompasses both assistance by a lawyer and dispensation from advance payment of the costs of proceedings.[1545]

Limits to Art. 47 CFR result from Art. 52(1) CFR. The test is therefore whether a proposed limitation touches upon the essence of the right or only limits a more peripheral element of the scope of protection. Limitations touching the periphery may be permissible if they pursue a legitimate public policy objective and are proportionate.[1546] The right to an effective judicial remedy has been the area in which the concept of essence and its violation has been most developed, particularly concerning personal data.[1547] Legislation that fails to provide individuals with the opportunity to pursue legal remedies for accessing their personal data, or for obtaining the rectification or erasure of such data, does not uphold the essence of the fundamental right to effective judicial protection, as enshrined in Art. 47 CFR.[1548] This results in certain extraterritorial effects, which require the EU to ensure that the same level of protection, including access to judicial review, must exist in third countries to which personal data originating in the EU are transferred.[1549]

1542 ibid.

1543 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.10.

1544 EU, 'Explanations Relating to the Charter of Fundamental Rights' (n 79), Article 47 - Right to an Effective Remedy and to a Fair Trial; Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para. 47.20.

1545 Case C-279/09 *DEB Deutsche Energiehandels- und Beratungsgesellschaft mbH v Bundesrepublik Deutschland* [2010] ECR I-13849, para 48.

1546 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559) para 47.190.

1547 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.194.

1548 *Schrems v Data Protection Commissioner*, (n 175) para 95; Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.194; Lock and Martin, 'Article 47 CFR' (n 885), para 20.

1549 *Schrems v Data Protection Commissioner* (n 175), para 96; Opinion 1/15 on the Draft Canada-EU PNR Agreement (n 541), paras 322 - 327; Lock and Martin, 'Article 47 CFR' (n 885), para 20.

Member States need "to protect the essential interests of their security and the guarantee of the procedural rights enjoyed by Union citizens"[1550] when deciding whether a restriction on the right to an effective remedy is proportionate. Thus, restrictions "must be counterbalanced by appropriate procedural mechanisms capable of guaranteeing a satisfactory degree of fairness in the procedure".[1551]

In the EU, the responsibility for providing effective judicial protection is shared between the EU and the Member States. Art. 19(1) TEU, which gives concrete expression to the rule of law affirmed in Art. 2 TEU, entrusts judicial review in the EU legal order to both the CJEU, composed of the ECJ, the General Court and specialised courts,[1552] and to national courts and tribunals.[1553] EU law protects the national procedural autonomy of the Member States subject to the principles of equivalence and effectiveness.[1554]

1550 Case C-300/11 *ZZ v Secretary of State for the Home Department* [2012], Opinion of AG Yves Bot, para 3.

1551 ibid, para 83; Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.207.

1552 The EU courts provide effective judicial protection against EU acts. The remedies that are relevant, primarily, in this regard are actions for annulment, TFEU, Art 263; actions for failure to act, TFEU, Art 265; actions for damages, TFEU, Art 246; and actions in staff cases, TFEU, Art 270. Further, indirect review under Art. 267 TFEU completes the judicial architecture, filling any gaps, according to Hans D Jarass, *Charta der Grundrechte der Europäischen Union, unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK: Kommentar* (3rd edn, CH Beck 2021), 417.

1553 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.27; *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* (n 1531), para 32; cf also *European Commission v Republic of Poland* (n 1531), para 47; Case C-192/18 *European Commission v Republic of Poland* [2019] OJ C 432/6, para 98; *A.K. v Krajowa Rada Sądownictwa and DO v Sąd Najwyższy* (n 1532), para 167; Mariolina Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (2016) 23 Maastricht Journal of European and Comparative Law 531, 537, states that as a "consequence of the separation of jurisdiction is that each judicial level is competent only for the acts emanating from the authorities falling within its jurisdiction, meaning that national courts would not be allowed to review the legality of measures issued by the European authorities or non-domestic national authorities, and similarly EU courts would not have jurisdiction to assess the legality of national administrative measures".

1554 Marcus Klamert, 'Treaty on European Union - Article 1 TEU' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (1st edn, Oxford University Press 2019); Marcus Klamert and Schima Bernhard, 'Treaty on European Union - Article 19 TEU' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU*

The Member States have to observe Art. 47 as well as the principle of sincere cooperation laid down in Art. 4(3) TEU.[1555] The CJEU interprets these requirements and thereby sets the EU standard regarding them. Apart from these requirements, EU law does not establish any general scheme governing remedies for its enforcement at the national level.[1556] It has long been established in CJEU case law that Member States have a positive obligation to offer "effective legal protection in the fields covered by Union law".[1557] Real effectiveness thus covers matters of procedural and substantive law.[1558]

Also, a requirement to ensure effective judicial remedies in multi-jurisdictional composite procedures has been, after long debate in the literature, explicitly recognised by the CJEU.[1559] This will be discussed in more detail below. In the Inuit case, the ECJ even recalled that the right to an effective remedy can, exceptionally, require the Member State bodies to create new remedies.[1560]

2. Judicial Remedies in the Eurodac and Interoperability Regulations

In this section, the study will examine which remedies the Eurodac and Interoperability Regulations provide. The discussion will begin with direct judicial remedies. It will then move on to examine indirect judicial remedies, including those found in the AMMR, Asylum and Return Directives, and at the EU level, where data-related issues could be addressed. This

---

Treaties and the Charter of Fundamental Rights: A Commentary (1st edn, Oxford University Press 2019); Lock and Martin, 'Article 47 CFR' (n 885), para 23.

1555 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.39.

1556 ibid, no 47.39.

1557 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.84.

1558 ibid, no 47.85.

1559 ibid, para 47.137; Case C-219/17 *Silvio Berlusconi, Fininvest v Banca d'Italia, Istituto per la Vigilanza Sulle Assicurazioni (IVASS)* [2018] OJ C 65/6, paras 44 and 46; cf also Herwig CH Hofmann, 'Multi-Jurisdictional Composite Procedures - The Backbone to the EU's Single Regulatory Space' [2019] SSRN Electronic Journal 26.

1560 Case C-583/11 *Inuit Tapiriit Kanatami and Others v European Parliament and Council, Kingdom of the Netherlands, European Commission* [2013] OJ C 344/14, para 104: "If the structure of the domestic legal system concerned were such that there was no remedy making it possible, even indirectly, to ensure respect for the rights which individuals derive from European Union law, or … of the sole means of access to a court was available to parties who were compelled to act unlawfully".

endeavour aims to determine whether the single direct judicial remedy in the Eurodac and Interoperability Regulations, which likely does not meet the effectiveness criteria outlined above, can be compensated for by indirect judicial remedies.

a) *Claims for Compensation*

The Eurodac Regulation as well as the Interoperability Regulations provide, as the only judicial remedy for individuals, the possibility to submit a claim for compensation in case a person has suffered damage from one of the systems in these Regulations. Since different authorities are responsible for different parts of Eurodac and the interoperability systems, claims must be addressed to the respective authority responsible for the specific part in the system that caused the damage.

aaa) *Eurodac Regulation*

With regard to Eurodac, it is Member States, eu-LISA, and the EBCG Agency that have different responsibilities. The Member State of origin is responsible for the process of taking and transmitting fingerprints, facial images, and other data.[1561] They have to secure the accuracy of the data as well as the lawfulness of the transmission and the recording, storing, correcting, and erasing of data.[1562] They must make sure that the results of fingerprint and facial image data comparisons are lawfully processed.[1563] Member States inform eu-LISA of security incidents detected on their systems.[1564] The Eurodac Regulation also permits, at the discretion of a Member State, the EBCG Agency teams or experts of the asylum support teams to take and transmit fingerprints to Eurodac on behalf of a Member State.[1565] Furthermore, besides national law enforcement agencies, Europol has access to Eurodac data.[1566] eu-LISA is, on the other hand, responsible

1561 Eurodac Regulation 2024.
1562 ibid, Art 36(1)(a), (b), (c).
1563 ibid, Art 36(1)(d).
1564 ibid, Art 48(3).
1565 ibid, Art 15(3), 22(8), 24(8) and 26(5).
1566 ibid, Art 7, 32 and 34.

for the technical management of Eurodac. The agency has to ensure that Eurodac is operated in accordance with the law.[1567]

According to Art. 52 Eurodac Regulation, only Member States are liable within the scope of their responsibilities. Any individual or Member State that has suffered material or immaterial damage due to unlawful processing operations or any actions that are incompatible with the Eurodac Regulation is entitled to compensation from the Member State responsible for the damage incurred.[1568] Claims for compensation are governed by the national law of the defendant Member State.[1569] If damage is caused by EBCG Agency personnel, the hosting Member State is responsible, as will be shown below. No compensation can be asked of Europol under the Eurodac Regulation. It will have to be made accountable for its actions based on the Europol Regulations.[1570] The reach of the compensation provision under the Eurodac Regulation is therefore quite limited.

According to the Eurodac Regulation, an action must be brought against the Member State that caused the damage. Unlike with other EU information systems, damages cannot be claimed from the state that acted on the basis of false information provided by another Member State.[1571] For instance, if a data subject was initially registered in Bulgaria with incorrect information and later files an asylum application in Germany, any damages suffered due to the inaccurately recorded data in Bulgaria would need to be claimed in Bulgaria. This restriction further limits the effectiveness of the compensation provision, as it makes this remedy less accessible in practice.

1567 ibid, Art 36(4).

1568 ibid, Art 52(1). The provision explains that the Member State is "exempted from its liability, in whole or in part, if it proves that it is not in any way responsible for the event giving rise to the damage"; ibid, Art. 52(2) further provides that "If any failure of a Member State to comply with its obligations under this Regulation causes damage to Eurodac, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State failed to take reasonable steps to prevent the damage from occurring or to minimise its impact".

1569 ibid, Art 52(3).

1570 Europol Regulation, Art 49ff.

1571 See for further discussions on claims for compensation under SIS II Regulation, Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553).

bbb) *Interoperability Regulation*

Similar to Eurodac, there are shared responsibilities with regard to the interoperability systems. Each Member State is responsible for the communication infrastructure of the ESP and the CIR. This includes managing and operating its existing national infrastructure, connecting to the interoperability components, manually verifying different identities, and ensuring compliance with data quality and security requirements under Union law and the database regulations.[1572] Europol is responsible for the processing of the queries of Europol data by the ESP.[1573] The ETIAS Central Unit, which is part of the EBCG Agency, is responsible for certain manual verifications of different identities.[1574] eu-LISA is responsible for the technical management of the central infrastructure of the interoperability components.[1575] The agency also has to ensure that the central infrastructures of the interoperability components are operated in accordance with the Interoperability Regulations.[1576] The agency has no access to any of the personal data processed through the ESP, the shared BMS, the CIR or the MID.[1577] eu-LISA, the ETIAS Central Unit, Europol, and the Member State authorities each have to ensure the security of the processing of personal data that takes place pursuant to the Interoperability Regulations.[1578]

Other than the Eurodac Regulation, the Interoperability Regulations provide that, within the realm of their responsibilities, the Member States, Europol, the EBCG Agency, and eu-LISA are liable.[1579] Any person, but also any Member State, that has suffered material or immaterial damage as a result of an unlawful processing operation or any other violation of the Regulation, is entitled to compensation from the responsible Member State, Europol, the EBCG Agency, or eu-LISA.[1580] They can exculpate themselves, wholly or in part, by proving that they are not responsible for the event that gave rise to the damage.[1581] Claims for compensation against a Member

1572 Interoperability Regulation - Judicial Cooperation, Art 56(1); Interoperability Regulation - Borders, Art 56(1).
1573 ibid, Art 57(1).
1574 ibid, Art 58(1).
1575 ibid, Art 55(1).
1576 ibid, Art 54(3).
1577 ibid.
1578 ibid, Art 42.
1579 ibid, Art 46(1).
1580 ibid, Art 46(1).
1581 ibid, Art 46(1).

State are governed by its national law. Claims for compensation against the controller or eu-LISA are subject to the conditions provided for in the Treaties.[1582]

The fact that, under the Interoperability Regulations, all actors can be held responsible – unlike under the Eurodac Regulation – facilitates access to justice. In practice, however, it may be difficult to identify who is responsible for specific harm, and data subjects may not always be able to determine where an error has occurred. Consider the following example: a data subject arrives in Greece and is subsequently granted asylum in Spain on the basis of family reunification. While travelling, the person is stopped and prevented from continuing their journey because the MID falsely indicates that they have committed identity fraud. Did the Greek authorities make a mistake when first recording data about the data subject? Or was the mistake the Spanish authorities', in a possible adjustment to the data, or during a manual comparison of data profiles? Did the error originate with eu-LISA, in the technical set-up of the automatic comparison of data profiles?

ccc) *Conditions for Compensation Claims in the EU*

The three main substantive conditions for the establishment of non-contractual liability are the same for the EU and the Member States. EU and state liability for damages were aligned by the ECJ in the case Bergaderm.[1583] With regard to data, the ECJ recently set out the requirements for compensation under the GDPR in the case IU v Österreichische Post AG.[1584] All in all, the ECJ provides for useful and clear criteria, naming

1582 ibid, Art 46(3); also, according to ibid, Art 46(2), if any failure of a Member State to comply with its obligations under the Interoperability Regulations causes damage to the interoperability components, that Member Sate is liable for such damage, unless and insofar as eu-LISA or another Member State bound by the Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

1583 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.247; Case C-352/98 P *Laboratoires pharmaceutiques Bergaderm SA and Jean-Jacques Goupil v Commission of the European Communities* [2000] ECR I-05291.

1584 Case C-300/21 *UI v Österreichische Post AG* [2023] OJ C 216/6; cf Felix Mikolasch, 'Requirements for GDPR Compensation after the ECJ Decision in UI v Österreichische Post' (*European Law Blog*, 11 September 2023) <https://europeanlawblog.

three cumulative requirements for compensation: a) infringement of a GDPR provision, b) a damage suffered, c) a causal link between the infringement and the damage.[1585] If the liability of EU institutions or bodies is at issue, a fourth condition needs to be satisfied, according to the CJEU's case law. In these cases, actual damage must be incurred to engage the non-contractual liability of the EU.[1586]

To be able to qualify for compensation, "the damage claimed must be of a certain significance".[1587] The ECJ found that in the context of Art. 82(1) GDPR, "the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation".[1588]

With regard to the second requirement, the Court clarified that the terms 'material or non-material damage' and 'compensation for the damage suffered' are autonomous concepts of EU law, as Art. 82 GDPR does not refer to Member State law. The wording and context of the provision, among

---

eu/2023/09/11/requirements-for-gdpr-compensation-after-the-ecj-decision-in-ui-v-osterreichische-post/> accessed 11 September 2023.

1585 *UI v Österreichische Post AG* (n 1584), para 32; cf also *Laboratoires pharmaceutiques Bergaderm SA and Jean-Jacques Goupil v Commission of the European Communities* (n 1583), para 42; Case C-611/12 *Jean-François Giordano v European Commission* [2014] OJ C 462/3, para 35; Case C-98/14 *Berlington Hungary Tanácsadó és Szolgáltató kft and Others v Magyar Állam* [2015] OJ C 270/10, para 104; Sophia Hassel, 'Non-Material Damages under the GDPR: What Do We Know so Far?' (*European Law Blog*, 4 March 2024) <https://europeanlawblog.eu/2024/03/04/non-material-damages-under-the-gdpr-what-do-we-know-so-far/>.

1586 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.249 with reference to *Laboratoires pharmaceutiques Bergaderm SA and Jean-Jacques Goupil v Commission of the European Communities* (n 1583), para 42; *Jean-François Giordano v European Commission* (n 1585), para 35; Case C-346/17 *Christoph Klein v European Commission* [2018] OJ C 399/9, para 60; Joined Cases C-447/17 P and C-479/17 P *Court of Justice of the European Union v Guardian Europe Sàrl and the European Commission and Guardian Europe Sàrl v the Court of Justice of the European Union and the European Commission* [2019] OJ C 383/8, para 147). She adds that "the test performed by the Court is still threefold as it combines the first two of the three conditions mentioned above. Under the usual formula of the Court, there needs to be, first, a sufficiently serious breach of a rule of EU law that is intended to confer rights on individuals (lawfulness of the conduct alleged); second, damage sustained by the injured party and third, a causal link between the damage and the action or inaction by the EU or Member State."

1587 *UI v Österreichische Post AG* (n 1584), para 13.

1588 ibid, para 42; the second instance court in Austria noted that, according to Austrian law, mere feelings of discomfort are not sufficient for compensation.

other aspects, should thus be taken into account for its interpretation.[1589] Doing this, the ECJ concludes that Art. 82(1) GDPR precludes a "national rule or practice" that requires non-material damages to reach a "certain degree of seriousness".[1590] This means that no threshold must be reached in order to achieve eligibility for compensation.[1591] Still, since damage is required for compensation, the Court states that a person affected needs to prove non-material damage.[1592] In the case Bindl v Commission, for the first time, the European Commission was ordered to pay compensation for moral damages for the improper transfer of personal data of an EU citizen to the United States.[1593]

Finally, the ECJ clarifies that "full and effective compensation"[1594] means that the damage is compensated in its entirety, without there being any need to require the payment of punitive damages.[1595] In consequence, the payment due under Art. 82(1) GDPR aims to make up for the damage

1589 ibid, para 29, 30.

1590 ibid, para 51; The context of the provision does not favour a threshold either. A "broad conception of 'damage'", as required by Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data [2016] OJ L119/1 (GDPR), Recital 146, would not be achievable if only damages that reach a 'certain degree of seriousness' were compensated (GDPR para 46). The ECJ adds that a threshold of seriousness could undermine a coherent GDPR application, as it would depend on each court to determine if such a threshold is met (para. 49). While the ECJ recalls that an 'autonomous and uniform definition specific to EU law' of concepts such as 'non-material damage' is required (GDPR, para. 42), it points out that Art. 82 GDPR does not contain any reference to any threshold of seriousness (GDPR, para. 45); Here, the ECJ departs clearly from the position of Case C-300/21 *UI v Österreichische Post AG* [2022], Opinion of AG Campos Sánchez-Bordona, para 105; Mikolasch, 'Requirements for GDPR Compensation after the ECJ Decision in UI v Österreichische Post' (n 1584).

1591 On the national level, however, it has been found that sometimes court will still introduce a threshold for compensation; cf Mikolasch, 'Requirements for GDPR Compensation after the ECJ Decision in UI v Österreichische Post' (n 1584).

1592 *UI v Österreichische Post AG* (n 1584), para 50.

1593 *Thomas Bindl v European Commission* (n 630), para 146; see for a more detailed analysis Sousa João Pedro 'Compensation for unlawful data transfers: The T-354/22 judgment (Bindl v. Commission) in perspective' (*OFFICIALBLOGUNIO*, 22 February 2025) <https://officialblogofunio.com/2025/02/22/compensation-for-unlawful-data-transfers-the-t-354-22-judgment-bindl-v-commission-in-perspective/>.

1594 GDPR, Recital 146.

1595 *UI v Österreichische Post AG* (n 1584), para 58.

suffered, not to punish a controller or processor.[1596] Both non-material and material damages need to be compensated independently of a specific level of intent or negligent conduct.[1597]

In connection with cases involving Eurodac data, the question arises as to whether the threshold of damage of "certain significance" will be reached. For example, is the damage significant when a data subject travels from Greece to Germany and is turned back because the Greek authorities did not inform them that fingerprints determine the country responsible for their asylum application? Maybe. In practice, however, data subjects will not enter proceedings to claim compensation in such or any similar scenario. First, because it would be nearly impossible to prove causality. Second, and more importantly, because asylum seekers and persons staying irregularly in the Schengen Area will likely only initiate proceedings that solve their core concern, i.e., to get protection in a (certain) Member State. They will hardly ever have the resources or the knowledge for proceedings beyond that. This fact is emphasised by the lack of cases of compensation in connection with Eurodac that could be found within this study's scope.[1598]

The CJEU has ruled, in several judgments, that violations of rights once committed may not be compensated by money alone, but that the lawful situation must then be restored.[1599] However, this position is contradicted by other judgments.[1600] The Court has no clear position, so far, on the

1596 Conceptually non-material damages are not limited to emotional and psychological harm. See, *inter alia,* GDPR, Recital 75; and any negative consequence may be compensated, as long as the damage is proven. Cf also *UI v Österreichische Post AG* (n 1584), para 50.

1597 Mikolasch, 'Requirements for GDPR Compensation after the ECJ Decision in UI v Österreichische Post' (n 1584): "This follows firstly from the GDPR that does not mention any such requirement in GDPR, Art 82(1) or 82(2). Secondly, the ECJ decision seems to confirm such an interpretation, as compensation should make up for the harm suffered by a natural person, disregarding therefore the subjective behaviour of a controller or processor (*UI v Österreichische Post AG* (n 1584), para 58). As an exception to this general rule, a controller or processor that proves not to be in any way responsible for the damage, for example in cases of *force majeure*, does not need to pay compensation, GDPR, Art 82(3)."

1598 Although it should be noted that the current case law only deals with the less extensive Eurodac system still in place at the time of writing.

1599 *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* (n 1529), para 19; *Unectef v Georges Heylens and others* (n 1127), para 14; Case C-24/00 *Commission of the European Communities v French Republic* [2004] ECR I-1277.

1600 Case 14/83 *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen* [1984] ECR I-1891, para 8ff; Case C-432/05 *Unibet (London) Ltd and Unibet (International) Ltd v Justitiekanslern* [2007] ECR I-2271.

question of whether Member States must provide more than compensatory remedies.[1601] As shown above, from the point of view of what data subjects under the Eurodac Regulation would want and need, the right to compensation (alone) cannot be considered an effective remedy.

At least according to the ECtHR, merely compensatory remedies are not sufficient if a violation is reversible.[1602] With regard to various rights, the ECtHR emphasises that a real violation must be prevented in the first place and that remedies must be available that can prevent or put an end to a violation. This is especially pertinent in relation to the non-refoulement obligation under Art. 3 ECHR.[1603] In cases where the processing of Eurodac data may result in a data subject being returned to a country where there is a risk of violating Art. 3 ECHR, a compensatory remedy is insufficient. The data subject must have the opportunity to challenge the Eurodac data before their return. If and how this is possible will be analysed in the next section.

b) *Indirect Judicial Review*

aa) National Level: Art. 43 AMMR, Asylum and Return Procedures

In most instances, data subjects only become aware that their data in Eurodac was recorded incorrectly or not at all upon receiving a decision, such as a transfer to another Member State following an asylum application. As demonstrated by the case law discussed in the preceding chapters, issues relating to Eurodac data are primarily addressed within the context of

1601 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 187ff; with reference to case law which argue that only monetary compensation does not suffice, *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* (n 1529), para 19; *Unectef v Georges Heylens and others* (n 1127), para 14; *Commission of the European Communities v French Republic* (n 1599), para 26; as well as cases that point in the other direction, *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen* (n 1600), para 8ff; *Unibet (London) Ltd and Unibet (International) Ltd v Justitiekanslern* (n 1600).

1602 In *Segerstedt-Wiberg and Others v Sweden* (n 864), para 121, official liability was not sufficient if and because it was not possible to obtain the complete deletion of a data collection in violation of Art. 8 ECHR; cf *Iatridis v Greece* ECHR 1999-II 75; cf also Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 215ff.

1603 *Jabari v Turkey* ECHR 2000-VIII, para 50; *Čonka and Others v Belgium* ECHR 2002-I, para 79.

transfer or return procedures. Remedies available in these procedures can therefore function as indirect judicial remedies for Eurodac data and may mitigate the limited scope of liability provisions discussed above.

The right to an effective remedy is contained in the various legal bases that guide asylum procedures. Art. 67(1) Asylum Procedure Regulation prescribes that applicants and persons subject to withdrawal of international protection have the right to an effective remedy before a court or tribunal, in connection with a decision rejecting an application, a decision withdrawing international protection and a return decision. Individuals recognised as eligible for subsidiary protection have the right to an effective remedy against any decision deeming their application for refugee status unfounded.[1604] According to Art. 13 Return Directive, the third-country national involved has the right to an effective remedy. This allows them to appeal against or seek a review of decisions related to their return before a competent judicial or administrative authority or a competent body composed of members who are impartial and who enjoy safeguards of independence. Both Directives also provide for the possibility of free legal assistance and representation in appeals procedures.[1605] Finally, Art. 43 AMMR provides for the right to an effective remedy, in the form of an appeal or a review, in fact and in law, against a transfer decision, before a court or tribunal. Other than under the Dublin III Regulation, this remedy has no suspensive effect, unless the Member State grants it.[1606] Depending on national law, Member States provide for a period of at least one week but no more than three weeks after the notification of a transfer decision within which the data subject concerned has to lodge the appeal.[1607] These changes vis-à-vis the Dublin III Regulation make access to justice considerably more difficult.[1608]

1604 Asylum Procedure Regulation, Art 67(2).

1605 ibid, Art 17, provides for free legal assistance and representation in the appeal procedure; Return Directive, Art 13 only states that Member States shall ensure that the necessary legal assistance and/or representation is granted on request free of charge in accordance with relevant national legislation or rules regarding legal aid, and may provide that such free legal assistance and/or representation is subject to conditions as set out in: Directive on Minimum Standards on Procedures in Member States for Granting and Withdrawing Refugee Status [2005] OJ L326/13.

1606 AMMR, Art 43(3).

1607 ibid, Art 43(2).

1608 It will be seen, whether the remedy holds up to the CJEU's requirements for an effective remedy (see to that effect, e.g, "It thus follows from the settled case-law of the Court that procedural rules governing actions for safeguarding the rights which individuals derive from EU law must not be any less favourable than those governing similar domestic actions (principle of equivalence) and must not be

Member States still have to ensure that legal assistance is granted on request free of charge where the person concerned cannot afford the costs involved.[1609] Regarding Art. 27 Dublin III Regulation, which was replaced by Art. 43 AMMR, the ECJ held that the remedy must be interpreted as ensuring that applicants for international protection have effective judicial protection by, inter alia, guaranteeing them the opportunity of bringing an action against a transfer decision. This action may concern the examination of the application of the Dublin III Regulation, including respect of the procedural guarantees laid down in it.[1610] The Court also held that only a single judicial remedy is required under the Dublin III Regulation, rather than multiple levels of jurisdiction.[1611] Additionally, no effective remedy needs to be provided against a decision made under the discretionary clause. A transfer decision can be implemented before a legal action against it has been resolved.[1612]

In these proceedings, as will be discussed in the following sections, questions regarding Eurodac data can be raised and addressed to some extent. However, two key issues emerge: first, how are Eurodac hits, security flags, or data transfers legally classified, and can they be appealed? As will be explored below, hits, flags, and data transfers can be classified as preparatory measures or 'purely factual conduct', making it difficult to challenge them through an appeal. The ECJ, in Samba Diouf, clarified that the absence of an appeal against a preparatory decision, such as conducting an asylum application under an accelerated procedure, does not breach Art. 47(1) CFR, as long as an appeal is available against the final decision.[1613] Secondly, it is not clear to what extent Member States are allowed to check the actions of other Member States, such as an entry in Eurodac. This will also be discussed further below.

---

framed in such a way as to render impossible in practice or excessively difficult the exercise of rights conferred by the legal order of the European Union (principle of effectiveness"), Case C-180/17 *X, Y v Staatssecretaris van Veiligheid en Justitie* [2018] OJ C 480/21, paras 34 and 35; Case C-194/19 *H.A v État belge* [2021] OJ C 217/3, para 42).

1609 AMMR, Art 43(4).

1610 *Tsegezab Mengesteab v Bundesrepublik Deutschland* (n 840), para 48; cf also *George Karim v Migrationsverket* (n 840), para 22.

1611 Case C-556/21 *Staatssecretaris van Justitie en Veiligheid v EN, SS, JY* [2023] OJ C 179/3, para 30.

1612 Case C-359/22 AHY *v Minister for Justice* (ECJ, 18 April 2024), para 47 and 61.

1613 Case C-69/10 *Brahim Samba Diouf v Ministre du Travail, de l'Emploi et de l'Immigration* [2011] OJ C 298/6, para 56.

It has to be added here that, even if there was a consensus on the above-mentioned questions, the extent to which different Member States grant review still varies.[1614] Especially under the Return Directive, no effective remedy in the sense of Art. 47 CFR is provided, since no 'tribunal' has to decide. In asylum procedures, the quality and effectiveness of a review vary. Art. 43 AMMR, in that sense, is a more robust remedy. It may be the one used most often with regard to Eurodac data questions. The curtailment of its effectiveness, especially by not having suspensive effect, should be viewed critically.

bb) EU Level: Preliminary Ruling

Under EU law, direct judicial review is possible according to Art. 263 TFEU. However, no action for annulment could be brought before the European courts: Eurodac cannot be considered as a body or organ of the EU. This is required by Art. 263 TFEU for an action for annulment to be admissible.[1615]

The lack of direct reviewability of Eurodac-related actions – such as hits, flags, information requests, and the provision of information – by European courts in an action for annulment could be seen as mitigated by the possibility of indirectly challenging these acts through a preliminary question of validity under Art. 267 TFEU.[1616] According to the case law of the CJEU, the range of measures that can be challenged indirectly through a question of validity is wider than those which are amenable to judicial review in direct actions, since it is held to include "all acts of the institutions without exceptions".[1617] This could imply that preliminary EU measures taken in the course of an information exchange procedure could be challenged in national proceedings directed at the challenge of the final

1614 Asylum Information Database and ECRE, 'Country Reports on Asylum in 23 Countries' (*asylumineurope.org*) <https://asylumineurope.org/reports/>; Boriss Cilevičs, 'Improving the Quality and Consistency of Asylum Decisions in the Council of Europe Member States' (Committee on Migration, Refugees and Population 2009) Doc. 1190; however, this is supposed to change to some degree with the introduction of the Asylum Procedure Regulation.

1615 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 542, fn 45.

1616 ibid 543.

1617 Case C-322/88 *Salvatore Grimaldi v Fonds des maladies professionnelles* [1989] ECR I-4407, para 8.

national measure.[1618] Such a conclusion is supported by the CJEU's Tillack case, in which the applicant tried to challenge the transfer of information from the European Anti-Fraud Office (OLAF) to the competent national authorities at the European level.[1619] While the Court of First Instance ruled that the transfer itself could not be considered a reviewable act, it acknowledged concerns that this conclusion might deprive the applicant of effective judicial protection. The Court noted that the applicant could still bring an action before the national court and request that the court seek a preliminary ruling from the CJEU.[1620]

A question for preliminary ruling could also emerge in the future, with reference to provisions of the Interoperability or Eurodac Regulations. For instance, a national court could request clarification on whether the existing legal remedies and procedural guarantees available to a data subject – allowing them to appeal before a national court against a criminal or administrative measure (such as an expulsion order) based on data retained or shared via interoperable databases by a foreign law enforcement or immigration authority – are compatible with the right to effective judicial protection under Art. 47 CFR.[1621]

3. Extrajudicial Remedies in the Eurodac and Interoperability Regulations

The Eurodac and Interoperability Regulations, but also the GDPR, provide the possibility for data subjects to request access to, rectification, or erasure of personal data from a Member State.[1622] The Regulations do not specify which authority within a Member State is responsible for a complaint against a decision or final administrative act by the Member State regarding such a request. As Art. 77 GDPR guarantees a right to lodge a complaint with a supervisory authority, this is possible under Art. 43 Eurodac Regulation and Art. 48 Interoperability Regulations, if the Member State does

1618 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 544.

1619 Case T-193/04 *Hans-Martin Tillack v Commission of the European Communities* [2006] ECR II-3995; Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 544.

1620 *Hans-Martin Tillack v Commission of the European Communities* (n 1619), para 80.

1621 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 531.

1622 Eurodac Regulation 2024, Art 43; Interoperability Regulation - Judicial Cooperation, Art 48.

not provide for another (judicial) remedy. National supervisory authorities are not considered tribunals[1623] and, as such, cannot provide an effective remedy within the meaning of Art. 47 CFR. The relevance of this conclusion to Art. 13 ECHR will be examined in more detail below. Nevertheless, a decision by a national supervisory authority can be appealed before a national court.[1624] It has to be examined whether this legal route, as a whole, might fulfil the criteria for effectiveness.

a) *Complaints before the Data Protection Authorities*

The development of non-judicial, administrative remedies as a means of resolving disputes concerning information processing without the intervention of a national court has been fostered since the inception of EU data protection law.[1625] The competence of a supervisory authority to perform the task of hearing complaints is derived directly from EU law: Art. 8(3) CFR and Art. 16 TFEU. Art. 8(3) CFR enshrines the role of the "independent authority"[1626] that is given the task of controlling compliance with data protection rules. The ECJ has stressed the importance of ensuring this control "by an independent authority of compliance".[1627] The determination of the procedural framework for receiving and handling complaints falls within the procedural autonomy of Member States, to the extent that no special

1623 They do not provide judicial review. For the conditions of what qualifies as tribunal see *François De Coster v Collège des bourgmestre et échevins de Watermael-Boitsfort* (n 1531), para 10; *Torresi v Consiglio dell'Ordine degli Avvocati di Macerata* (n 1531), para 17; *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* (n 1531), para 38; *European Commission v Republic of Poland* (n 1531), para 55; On the concept of a court or tribunal and the autonomy of EU law, see *Slowakische Republik v Achmea BV* (n 1531); Opinion 1/17 On the EU-Canada CETA Agreement (n 826).

1624 GDPR, Art 78.

1625 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 400; cf Data Protection Directive 95/46/EC.

1626 cf TEU, Art 16.

1627 *Digital Rights Ireland Ltd v Minister for Communications and Others* (n 730) para 68; Waltraut Kotschy, 'Article 77 - Right to Lodge a Complaint with a Supervisory Authority' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 1121.

provisions are foreseen under EU law.[1628] In connection with Eurodac data, procedural and substantive provisions are found in the GDPR, which constitutes *lex generalis*, and the Eurodac Regulation – particularly Art. 43 – which is considered *lex specialis*.[1629] The same goes for the Interoperability Regulations; they provide, in Art. 48, an extrajudicial remedy, which refers to the GDPR.[1630]

The role of national supervisory authorities in overseeing the lawfulness of the processing is crucial and an "essential correlate of the rule of law."[1631] As Vavoula and Marsch have pointed out, this is all the more necessary in the case of Eurodac, which stores a special category of personal data – biometric data – collected from a particularly vulnerable group of individuals.[1632] Consequently, the same goes for the interoperability systems that also store biometric data.

aa) Eurodac Regulation

The Eurodac Regulation mandates supervision of compliance with data rights by both national supervisory authorities and supranational data protection authorities.[1633] The monitoring of the national authorities is

1628 Kotschy, 'Article 77 - Right to Lodge a Complaint with a Supervisory Authority' (n 1627) 1121.

1629 See chapter: The Right to Information; Eurodac Regulation 2024, Recital 77; Interoperability Regulation - Judicial Cooperation, Recital 53.

1630 See for the establishment of the Data Supervisory Authority, Interoperability Regulation - Borders, Art 51; Interoperability Regulation - Judicial Cooperation, Art 51.

1631 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564), 400; with reference to Nikolaus Marsch, 'Networks of Supervisory Bodies for Information Management in the European Administrative Union' (2014) 20 European Public Law 127.

1632 cf Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564), 400; with reference to Marsch, 'Networks of Supervisory Bodies for Information Management in the European Administrative Union' (n 1631); also Secretariat of the Eurodac Supervision Coordination Group, 'Eurodac Supervision Coordination Group: Activity Report 2016-2017' (European Data Protection Supervisor 2019).

1633 Eurodac Regulation 2024, Art 44 - 46; Marsch understands this approach as vertical centralisation, in cf Marsch, 'Networks of Supervisory Bodies for Information Management in the European Administrative Union' (n 1631) 143; cf also Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and*

entrusted to national supervisory authorities.[1634] While national 'independent public authorities', according to Art. 41(1) Police Directive, have to monitor the lawfulness of the processing of personal data in the national law enforcement context,[1635] processing of personal data by Europol is supervised by the EDPS in accordance with the Europol Regulation.[1636] The supervision of EU institutions concerning Eurodac, in particular by eu-LISA, is bestowed on the EDPS.[1637] It provides an audit of eu-LISA's activities every three years.[1638]

The supervisory authorities on both levels have to cooperate with each other and meet at least twice a year in the Eurodac Supervision Coordination Group. The latter provides a joint report of activities that is sent to the European Parliament, the Council, the Commission, and eu-LISA every two years.[1639] Internally, eu-LISA is further supervised by its Data Protection Officer, who receives complaints concerning actions of eu-LISA affecting individuals.[1640]

bb) Interoperability Regulation

Similar to the Eurodac Regulation, the Interoperability Regulations require both national and supranational data protection authorities to oversee compliance with data rights.[1641] National supervisory authorities are responsible for monitoring national authorities. They conduct audits every four years and submit annual reports detailing requests for rectification, erasure, or restriction of data.[1642]

The EDPS monitors the EU institutions. It has to ensure that an audit of personal data processing operations by eu-LISA, the ETIAS Central

Justice: Towards Harmonised Data Protection Principles for Information Exchange At EU-Level (n 542).

1634 Eurodac Regulation 2024, Art 44.
1635 ibid, Art 47(1); in conjunction with Police Directive, Art 41(1).
1636 Eurodac Regulation 2024, Art 47(2) and Europol Regulation.
1637 Eurodac Regulation 2024, Art 45.
1638 ibid, Art 45(2).
1639 ibid, Art 46(4).
1640 eu-LISA Regulation, Art 18(2)(a).
1641 Interoperability Regulation - Judicial Cooperation, Art 51, 52 and 53; Interoperability Regulation - Borders, Art 56(1).
1642 ibid, Art 51(1), (2).

Unit, and Europol is carried out at least every four years.[1643] The national supervisory authorities and the EDPS cooperate within the framework of their respective responsibilities.[1644]

b) *Tasks of the Data Protection Authorities under the GDPR*

Art. 43(5) Eurodac Regulation and Art. 48(8) Interoperability Regulation particularise the right to lodge a complaint with a competent or supervisory authority, as guaranteed in Art. 77 GDPR. Whenever a Member State does not agree with a request for access, rectification, or erasure of data exercised by a data subject, they have to provide the data subject with information on how to bring an action or complaint.[1645] The Eurodac and Interoperability Regulations do not specify what 'action' or 'complaint' has to be provided by the Member States. The remedies and procedural guarantees are primarily set out in the GDPR, which is, as *lex generalis*, applicable.

The GDPR lists, amongst the tasks of the national supervisory authorities, the handling and investigation of complaints lodged by a data subject.[1646] The procedures before the national supervisory authorities are free of charge and submission forms have to be provided by the state.[1647] National supervisory authorities have encompassing investigative powers. They can order the controller and processor to provide any information it requires for the performance of its tasks.[1648] National supervisory authorities also have a range of corrective powers. They cannot only issue reprimands. They may order the controller or the processor to comply with the data subject's requests to exercise their rights or to bring processing operations into compliance with the law and even, where appropriate, in a specified manner and within a specified period.[1649] Furthermore, they can impose a temporary or definitive limitation, including a ban on processing.[1650] Finally, national supervisory authorities have the power to bring

1643 ibid, Art 52.
1644 ibid, Art 53.
1645 Eurodac Regulation 2024, Art 43(5); Interoperability Regulation - Judicial Cooperation, Art 48(8); Interoperability Regulation - Borders, Art 48(8).
1646 GDPR, Art 57(1)(f).
1647 ibid, Art 57(2) and (3).
1648 ibid, Art 58(1)(a).
1649 ibid, Art 58(2)(b) - (d).
1650 ibid, Art 58(2)(f).

data protection law infringements to the attention of the judicial authorities. Where appropriate, they may commence or engage otherwise in legal proceedings in order to enforce the law.[1651]

With regard to Eurodac, decisions or the final administrative act under review are very often the result of the input of administrative actors of different Member States.[1652] In case of such cross-border processing operations, one lead supervisory authority coordinates and handles a case.[1653] In cases where the subject matter pertains solely to an establishment within a Member State, or where the issues significantly affect data subjects exclusively within that Member State, the supervisory authority of that Member State is responsible for handling the complaint.[1654]

Lodging a complaint before a national supervisory authority cannot be considered an effective remedy in the sense of Art. 47 CFR. As discussed above, under the CFR, the intervention of a 'tribunal' in accordance with Art. 267 TFEU is necessary. National supervisory authorities do not fulfil these criteria,[1655] in particular because they cannot provide judicial review[1656] as non-judicial authorities.[1657]

Under Art. 13 ECHR, complaints before a national supervisory authority could potentially be considered an effective remedy: non-judicial remedies can be considered effective if the authority's powers and the procedural

1651 ibid, Art 58(5).

1652 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 403; Micaela Lottini, 'From "Administrative Cooperation" in the Application of European Union Law to "Administrative Cooperation" in the Protection of European Rights and Liberties' (2012) 18 European Public Law 127, 135.

1653 GDPR, Art 56(1).

1654 ibid, Art 56(2).

1655 cf Laurent Pech, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Publishing 2021), no 47.325ff and fn 129.

1656 Which is ultimately, what is required under Art. 47 CFR, cf Lock and Martin, 'Article 47 CFR' (n 885), para 4; Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), no 47.17; *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530), para 52; Joined Cases C-245/19 and C-246/19 *État luxembourgeois v B and État luxembourgeois v B, C, D and F.C.* [2020] OJ C 414/6, paras 52 - 57.

1657 In *Ligue des droits humains* (n 876) para 55 the ECJ decided, with regard to access under the Police Directive, that data subjects must have an effective judicial remedy against the decision of a supervisory authority.

safeguards provide enough security and fairness.[1658] National supervisory authorities have the power to order authorities to behave in a certain way or comply with the law. In that sense, their decisions are binding.[1659] They can furthermore request information from authorities and have encompassing investigative powers. This might allow for 'rigorous scrutiny', as required by the ECtHR, in cases where a violation of Art. 3 ECHR is at issue.[1660] However, in procedures before national supervisory authorities, no legal aid or representation is guaranteed, other than the provision of submission forms.[1661] National supervisory authorities have no power to suspend administrative actions,[1662] such as a return decision, by another administrative body. They therefore cannot really grant 'appropriate relief'.[1663]

In summary, while Art. 57 and Art. 58 GDPR establish a comprehensive and mandatory list of tasks and powers for supervisory authorities – drawing inspiration from the EDPS under Regulation 45/2001,[1664] which significantly enhanced the data protection rights of individuals in the EU – complaints regarding Eurodac data submitted to a national supervisory authority cannot be deemed an effective remedy under Art. 47 CFR or Art. 13 ECHR. As will be discussed below, decisions by national supervisory authorities can, however, be appealed before a national court.

4. Penalties

As part of their responsibilities, Member States have to take the necessary measures to ensure that any processing of data entered in Eurodac contrary to the purposes of the Eurodac Regulation is punishable by penalties. This includes administrative and/or criminal penalties in accordance with

1658 ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), para 29; with reference to *Klass and Others v Germany* (n 1500), para 67; *Silver and Others v United Kingdom* (n 1501), para 113; *Kudla v Poland* (n 1492), para 157; *Mugemangango v Belgium* (n 1501), para 67.

1659 As required under ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827), para 30.

1660 cf *M.S.S v Belgium and Greece* (n 1468), para 293, with further references.

1661 GDPR, Art 58.

1662 As required by the ECtHR, cf *E.H. v France* (n 1418), para 177; *S.K. v Russia* (n 1522), para 81, etc.

1663 cf *Boyle and Rice v. the United Kingdom* (n 1499), para 52; *Powell and Rayner v United Kingdom* (n 1504), para 31; *M.S.S v Belgium and Greece* (n 1468), s 288.

1664 Kotschy, 'Article 77 - Right to Lodge a Complaint with a Supervisory Authority' (n 1627) 1120.

national law which have to be effective, proportionate, and dissuasive.[1665] The same applies within the Interoperability systems: Member States are obliged to ensure effective, proportionate, and dissuasive penalties in accordance with their national law in case of misuse of data.[1666]

Penalties do not provide a right for data subjects. Data subjects can, in accordance with national law, alert authorities of data misuse. Still, they have no right to make sure that a person will indeed be punished. They also possess no rights in a potential procedure that leads to a penalty, unless the state decides to provide for it.

The Eurodac and Interoperability Regulations thus do not contain any effective remedy for Eurodac data subjects. This observation will be confirmed in the next chapters, where case law is studied. Relevant case law with regard to Eurodac data so far exists primarily from appeals against transfer decisions according to Art. 27 Dublin III Regulation (replaced by Art. 43 AMMR). Numbers for access, rectification, or erasure requests through the national supervisory authorities are continuously low, albeit rising,[1667] and, as far as the research in this study provides, are in general not appealed in a court.

5. Remedies According to the GDPR

As seen above, extrajudicial legal routes do not provide an effective remedy. The national supervisory authority's decisions can be appealed before a national court. According to Art. 78 GDPR, every natural or legal person has the right to an effective judicial remedy against a legally binding decision made by a supervisory authority concerning them. This right also applies if the supervisory authority fails to address a complaint or does not inform the data subject about the progress or outcome of the complaint within three months.

It is questionable whether an effective remedy is even possible at this stage with regard to certain cases on Eurodac data. If an administrative procedure is underway, in which the Eurodac data in question are used, such as an asylum or return procedure, then this legal route must be considered as being too long. The data subject would first have to, e.g., in case

1665 Eurodac Regulation 2024, Art 59.
1666 Interoperability Regulation - Judicial Cooperation, Art 45.
1667 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 25.

of inaccurate data, request rectification from the national administrative authority (e.g., the migration office), then the national supervisory authority would have to decide; only at the third instance, the national court, would an effective remedy be available. Promptness, which is an important element under Art. 13 ECHR[1668] and Art. 47 CFR,[1669] is not granted this way. Furthermore, none of the remedies so far would have had suspensive effect.

The GDPR provides a quicker legal procedure with Art. 79 GDPR, stipulating that a right to an effective judicial remedy must be provided in relation to decisions by the "controller" or the "processor" of personal data, which is the Member States processing Eurodac data as well as the supervisory authority. According to the ECJ, data subjects have the option to exercise the remedies provided for in Art. 77(1) and Art. 78(1) GDPR, on the one hand, and Art. 79(1) thereof, on the other, concurrently with and independently of each other.[1670] According to the ECJ, providing multiple remedies reinforces the objective outlined in Recital 141 of the GDPR: every data subject who believes their rights under the regulation have been violated has the right to an effective judicial remedy, in accordance with Art. 47 CFR.[1671] It is, however, for the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies.[1672]

1668 *Paulino Tomás v Portugal* (n 1506); *Çelik and İmret v Turkey* (n 1506), para 59.

1669 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.10; Lock and Martin, 'Article 47 CFR' (n 885), para 31.

1670 Case C-132/21 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2023] OJ C 71/6, para 57; Advocate General observed in point 55 of his Opinion that A number of conclusions can be drawn from an interpretation of Article 15(1)(h) of the GDPR read in the light of Recitals 58 and 63 of that regulation. First, it is apparent that the EU legislature was fully aware of the conflicts that could arise between the right to protection of personal data guaranteed by Article 8 of the Charter and the right to protection of intellectual property under Article 17(2) of the Charter. Second, it is clear that its intention was not to sacrifice one fundamental right for another. On the contrary, further analysis of the provisions of the GDPR indicates that it wished to ensure a fair balance between rights and responsibilities (Case C-132/21 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2022] OJ, Opinion of AG Richard Tour, point 55).

1671 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* (n 1670), para 44.

1672 ibid, para 57.

In Switzerland, for example, an order by the State Secretariat for Migration[1673] to reject a request for data rectification may be appealed directly to the Federal Administrative Court.[1674] EU Member States may offer similar routes of judicial review. However, the Eurodac and Interoperability Regulations themselves do not provide for an effective remedy, which means that data subjects within the EU experience different levels of protection and, in the worst case, may have no access to an effective legal remedy.

6. Scope and Challenges of Effective Remedies under Eurodac and the Interoperability Systems

The first part of this section addresses key procedural challenges. These include the involvement of multiple national authorities from different countries, the types of acts that can be challenged – such as a Eurodac hit or a security flag – and the nature of evidence that must be provided, and by whom. The second part examines challenges to the right to an effective remedy that are specific to procedures involving Eurodac data. Finally, the section considers specific administrative acts and decisions, assessing whether an effective remedy exists against them.

a) *Reviewing Acts by Other Member States*

The potentially simultaneous involvement of a multitude of national or European authorities in interoperable information systems raises serious issues of transparency as to which administration is to be held responsible for a particular action or decision. This in turn renders it even more difficult to ensure the accountability of the overall information-sharing framework.[1675]

1673 According to Asylverordnung 3 über die Bearbeitung von Personendaten [1999] SR 142.314 (AsylV 3), Art 11(a).

1674 According to Bundesgesetz über das Bundesverwaltungsgericht [2005] SR 173.32 (VGG), Art 31; the Federal Administrative Court assesses appeals against rulings in accordance with Federal Act on Administrative Procedure [1968] SR 172.021 (APA - Switzerland) (Bundesgesetz über das Verwaltungsverfahren (VwVG)), Art 5. The rejection of an application for rectification would likely qualify as an order in the sense of APA - Switzerland, Art 5.

1675 Curtin and Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55), 64; Jens-Peter Schneider, 'Information Exchange and Its Problems' in Carol Harlow, Päivi Leino and Giacinto della

We thus have to examine whether, and to what extent, acts or decisions of other Member States can be subject to review. If (judicial) review is not possible, this constitutes a significant obstacle for data subjects seeking effective access to justice.

aa) Composite Procedures within the EU

The traditional national system of judicial review is challenged in procedures using Eurodac data: in many cases, the final administrative act under review is the result of information from different jurisdictions and the input of administrative actors of different Member States.[1676] This makes Eurodac an example of composite information management.[1677] Consequently, one may ask: how and to what extent can authorities of one Member State review acts of an authority of another Member State? What procedural

Cananea (eds), *Research Handbook on EU Administrative Law* (Edward Elgar 2017) 103ff.

1676 cf Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 403; Alexander Türk, 'Chapter 9: Judicial Review of Integrated Administration in the EU' in Alexander Türk and Herwig CH Hofmann (eds), *Legal Challenges in EU Administrative Law: Towards an Integrated Administration* (Edward Elgar 2009); Lottini, 'From "Administrative Cooperation" in the Application of European Union Law to "Administrative Cooperation" in the Protection of European Rights and Liberties' (n 1652) 135.

1677 Some legal scholars define composite procedures as "decision-making process involving both national and Union administrations", stating that the final decision in such procedures requires the active participation of both levels (Christina Eckes and Raffaele D'Ambrosio, 'Composite Administrative Procedures in the European Union' (European Central Bank 2020) No. 20). According to this opinion, Eurodac procedures would not count as composite procedures. However, this study follows the opinion of Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.140ff, who differentiates four basic constellations of composite procedures. First, where relevant procedures establish an EU institution or body as author of a final decision on the basis of non-binding input from national actors; second, where EU procedural rules establish that the final decision is taken by a national authority, either because an EU institution or body has only given input into the decision-making procedure or because the EU institution is bound by a national act; third (which is what is looked at in this study), procedures where several Member State authorities act together in one procedure in the scope of EU law; and fourth, where a Member State act has an effect not only under national law but also under EU law; See for a more extensive analysis Hofmann, 'Multi-Jurisdictional Composite Procedures' (n 1559).

standards do they have to adhere to, if they have to make a decision on a matter in which other Member State authorities were involved?

National courts within the EU are, in principle, competent to review only acts emanating from the authorities falling within their jurisdiction.[1678] This means that national courts are, notionally, not allowed to review the legality of measures issued by the European authorities or non-domestic national authorities. Similarly, EU courts do not have jurisdiction to assess the legality of national administrative measures.[1679] Whether this separation is strictly implemented and makes sense within multi-jurisdictional composite procedures, is discussed below.

Furthermore, as has been mentioned above, Member States enjoy procedural autonomy where there are no harmonised procedural rules, provided that they respect Art. 47 CFR rights and obligations.[1680] Apart from these requirements, EU law does not establish any general scheme governing remedies for its enforcement at the national level.[1681] Certain procedural principles for composite proceedings have been developed in case law and must be observed. In the context of data exchange especially, this is the duty of care.[1682] In its case, TU München, the ECJ developed the formula

1678 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 537; TEU, Art 19, provides that the responsibility for providing effective judicial protection is shared between the EU and the Member States. The scope of application of Art. 19(1) TEU is broader than that of CFR, Art 47, as it relates to the 'fields covered by Union law'. Article 19(1) can therefore be applicable even if the Member States are not implementing EU law in the sense of Article 51(1) of the Charter (Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), no 47.38); Burkhard Hess and Pietro Orlotani (eds), *Impediments of National Procedural Law to the Free Movement of Judgments*, vol 1 (Bloomsbury Publishing 2019) 9ff discuss the question of specialised judges in cross-border (civil law) cases.

1679 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 537.

1680 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.39; as well as the principles of effectiveness and equivalence the Rewe-principles and the principle of sincere cooperation laid down in TEU, Art 4(3); cf also Anna Ghavanini, 'Towards an EU Law Doctrine on the Exercise of Discretion in National Courts? The Member States' Self-Imposed Limits on National Procedural Autonomy' (2016) 53 Common Market Law Review 339, 342.

1681 Rauchegger, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 1524), para 47.39.

1682 Herwig CH Hofmann, 'The Duty of Care in EU Public Law – A Principle Between Discretion and Proportionality' (2020) 13 Review of European Administrative Law 87.

for identifying the duty of care as "the duty of the competent institution to examine carefully and impartially all the relevant aspects of the individual case".[1683] In the context of data exchange, the principle of duty of care requires that the administration collects all necessary information and conducts a thorough factual assessment of that information.[1684] To be able to evaluate compliance with the duty of care in information networks, the decision-making process must be so transparent as to reflect the various stages of information assessment.[1685] The role and obligations of each network member in the decision-making process must be identifiable.[1686] In its case, Commission v Kingdom of Spain, the ECJ held, in the context of the SIS, that both the authorities of the state taking the final measure as well as the authorities of the state entering the alert into the system were obliged to verify the conditions of refusal to grant entry into the Schengen Area.[1687]

Another procedural principle that has to be adhered to in composite procedures is the right to be heard. In composite procedures, the assessment of facts on the one hand, and the adoption of a final act or decision on the other hand, are functions often dissociated and allocated to authorities in different jurisdictions.[1688] According to the definition of the CJEU, the right to be heard is a general principle of EU law. It requires compliance by EU and national bodies when acting in the scope of EU law.[1689] The right is effective whenever a person adversely affected by a decision is in a position to espouse their views before the authority that determines the substance of the final act. Consequently, if secondary legislation does not explicitly provide for it, it may prove difficult to determine before which

1683 *Technische Universität München v Hauptzollamt München-Mitte* (n 1298), para 14.

1684 Morgane Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (2014) 20 European Public Law 147, 150.

1685 ibid 150.

1686 ibid.

1687 Case C-503/03 *Commission of the European Communities v Kingdom of Spain* [2006] ECR I-1097, paras 52 and 55.

1688 Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684) 151.

1689 Case 17/74 *Transocean Marine Paint Association v Commission of the European Communities* [1974] ECR 1063; Case C-135/92 *Fiskano AB v Commission of the European Communities* [1994] ECR I-2885; Case T-450/93 *Lisrestal - Organização Gestão de Restaurantes Colectivos Ld*[a] *and others v Commission of the European Communities* [1994] ECR II-1177; This right is also protected under CFR, Art 41(2) first indent, but limited to actions by institutions, bodies, offices and agencies of the Union.

authority to state one's views.[1690] In various decisions the CJEU decided, with regard to composite procedures between Union and national bodies, that a person has to be able to make their views known in front of the Union administrative body which hears the case.[1691] Alternatively, this body has to take into consideration what the person has stated before a previous national body for its final decision.[1692] It is argued here that this case law should also be applicable in procedures where no Union body is involved, since the right to be heard must be equally respected by national bodies.

This means that there are some procedural principles a person can insist on in composite proceedings. In the context of Eurodac, a data subject must be heard on issues with Eurodac data, e.g., that a certain data item is inaccurate. The national authority also must be able, based on their duty of care, to evaluate each stage of information assessment and verify the data if they affects the final measure they are taking, even if the data collection took place in another Member State.

The question remains: can a Member State can review another Member State administration's action or decision? In the realm of EU migration information systems, there is at least one case at the national level, the Forabosco case, where the French Council of State (*Conseil d'Etat*) reviewed the lawfulness of a German SIS alert on the basis of the Schengen Convention.[1693] The decision concerned a visa application. The French Council of State considered that the entry ban entered in the SIS database due to a negative asylum decision was not a sufficient reason to refuse a long-stay visa.[1694] Tidghi has argued that such an approach could equally be adopted by any other court faced with the same alert, on the basis of the Schengen Convention.[1695] Eliantonio pointed out that this may well remain an isolated case and is certainly not a precedent that can provide sufficient legal certainty as to the reviewability of information provision measures issued

1690 Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 16384) 151; with reference to Case T-114/99 *CSR PAMPRYL v Commission of the European Communities* [1999] ECR II-3331; cf also Conseil d'État, 2/1 SSR, du 21 mars 2001, 202694 202695 202696, mentionné aux tables du recueil Lebon.

1691 *Technische Universität München v Hauptzollamt München-Mitte* (n 1298).

1692 *Case T-346/94 France-aviation v Commission of the European Communities* [1995] ECR II-2841.

1693 Conseil d'État, 2/6 SSR, du 9 juin 1999, 190384, publié au recueil Lebon.

1694 ibid.

1695 Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684) 158.

in the context of SIS.[1696] In a similar situation, another judge might in the future seek interpretation of EU law under the preliminary reference mechanism.[1697]

The case law on composite procedures has, to date, been evolving on a case-by-case basis, non-exhaustively addressing individual constellations only.[1698] Case law from areas of law beyond migration information systems is worth examining, as it can provide valuable insights for future Eurodac cases. In the Berlioz case, which concerned the exchange of information upon request between tax administrations, the ECJ held that the right to an effective judicial remedy under Art. 47 CFR requires that one national administration, and subsequently its courts on review, must be able to review another Member State administration's decision.[1699] The ECJ established, for the first time, that the basis of that review will not be compliant with the other Member State's law. Yet, it is compliant with the requirements established by the EU directive, confirming the possibility of a composite procedure that links various national administrations in the field of taxation.[1700,1701] This solution allows for a review by the courts and tribunals of one Member State of the actions of another Member State's administration against an EU standard, which constitutes a central innovation for ensuring effective remedies.[1702] In the case of État Luxembourgeois, the ECJ clarified that the right to an effective review entails that the criterion of mutual review applies not only to the specific legislative act, such as an EU

1696 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 542.

1697 Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684) 157.

1698 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.138; Case C-219/17 *Silvio Berlusconi, Fininvest v Banca d'Italia, Istituto per la Vigilanza Sulle Assicurazioni (IVASS)* [2018] Opinion of AG Campos Sánchez-Bordona, paras 58 - 79, with a full review of the case law pre-dating Berlusconi and the literature on the matter.

1699 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530).

1700 Council Directive on Administrative Cooperation in the Field of Taxation [2011] OJ L64/1.

1701 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530), paras 56 and 78 - 89.

1702 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.145.

directive, but also to compliance with EU fundamental rights and general principles.[1703]

This case law might not be applicable in Eurodac-related cases. Still, Mazzotti and Eliantonio have suggested that the Berlioz case could amount to an authority liable to be extended to horizontal composite procedures in general.[1704] Moreover, because many questions in this area of law have not been conclusively clarified, the above arguments should at least be put forward in order to expand legal protection for data subjects in Eurodac cases.

bb) Reviewing Preparatory Acts or 'Factual Conduct' (by Other Member States)

In many cases concerning Eurodac data, the key issue is not whether a Member State can review a decision made by another Member State, but rather whether a hit, a security flag, or an exchange of information from another Member State is reviewable. Therefore, the following section first examines how these acts should be legally qualified. In a second step, the study addresses whether they are subject to review.

aaa) *Qualifying Information Sharing, Hits and Security Flags*

In the context of migration information systems, two qualifications have been brought forward by scholars for Eurodac hits and alerts: 'purely factual conduct'[1705] or provisional, preparatory measures.[1706] It should be

1703 *État luxembourgeois v B and État luxembourgeois v. B, C, D and F.C.* (n 1656), para 111.

1704 Paolo Mazzotti and Mariolina Eliantonio, 'Transnational Judicial Review in Horizontal Composite Procedures: Berlioz, Donnellan, and the Constitutional Law of the Union' (2020) 5 European Papers - A Journal on Law and Integration 41.

1705 Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 64, qualified an Eurodac hit as 'purely factual conduct'.

1706 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 542; Mariolina Eliantonio, 'Judicial Review in an Integrated Administration: The Case of "Composite Procedures"' (2015) 7 Review of European Administrative Law 65, 70ff, referencing Case C-521/04 P (R) *Hans-Martin Tillack v Commission of the European Communities* (n 1619),

noted that the concept of 'purely factual conduct' (Realakte) refers to a particular form of administrative action which, in the classification adopted here, is primarily recognised in the German and Swiss legal systems.[1707] 'Purely factual conduct' is administrative conduct that does not intend to have legal effects but merely to achieve a factual result.[1708] In other words, a 'Realakt' can be regarded as a working term for non-legally binding acts by an authority.[1709]

Preparatory measures[1710] may also be described as administrative action. They can be qualified as 'purely factual conduct', since they do not intend to have direct legal effects but merely to achieve a factual result,[1711] unless

suggests in the context of SIS II, that an SIS alert is a preparatory act; Schneider, 'Information Exchange and Its Problems' (n 1675) 104.

1707 While similar forms of administrative practice exist in other jurisdictions, they are categorised somewhat differently: In the Dutch legal system, e.g. while there is no explicit concept termed *Realakt* as in German or Swiss law, the notion of factual action (*feitelijke handeling*) serves a comparable role. Factual actions are administrative measures that do not produce legal consequences – for instance, informal acts like information notices or physical inspections – which therefore cannot be challenged before administrative courts. Instead, such acts must typically be pursued through civil courts, as they do not qualify as administrative decisions under Dutch law (see Verburg André & Schueler Ben 'Procedural Justice in Dutch Administrative Law Proceedings' (2014) 10(4) *Utrecht Law Review*, 56–72).

1708 In Switzerland, an administrative act exists only if the requirements in APA - Switzerland, Art 35 sentence 1 and APA - Switzerland, Art 5 respectively are fulfilled. According to this, an administrative act is any sovereign measure taken by an authority to regulate an individual case in the field of public law and which is aimed at having a direct legal effect on the outside. If one of these requirements cannot be affirmed the act is considered 'purely factual conduct'. In practice, 'purely factual conduct' is often assumed when an administrative action has no regulatory effect (Peter Karlen, *Schweizerisches Verwaltungsrecht: Gesamtdarstellung unter Einbezug des Europäischen Kontextes* (Schulthess 2018) 194); in Germany too, 'purely factual conduct' is understood to be actions that are not ultimately aimed at bringing about certain legal consequences, but at bringing about an actual result (Barbara Remmert, 'Schlichtes Verwaltungshandeln' in Hans-Uwe Erichsen and Dirk Ehlers (eds), *Allgemeines Verwaltungsrecht* (De Gruyter 2005), § 35 I 5).

1709 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 1 and 8 with reference to case law: "This is because the Court of Justice has made the characteristic 'legally binding' the decisive one in determining whether an act by the Union can be appealed."

1710 ibid, 63 uses the term 'vorbereitende Massnahmen'.

1711 See for a more in-depth discussion about preparatory measures, ibid, 63ff.

they themselves conclude a procedure.[1712] Preparatory measures are taken in anticipation of a decision by an authority of a Member State.[1713] In the context of the composite procedures, this categorisation looks specifically at which authority takes the final decision in the administrative decision-making proceedings.[1714] Composite procedures necessarily entail the participation of multiple authorities, belonging to the national or the EU system of administration. From this perspective, all activities, other than the taking of the final decision, whether stemming from a national or a EU authority, are of a preparatory nature in the decision-making process.[1715]

Information Sharing

The act of sharing information does not intend to have legal effect. It aims at a purely factual result: another authority shall gain access to the same information as the one that is sending it. Information sharing is not a legally binding administrative act or decision. Information sharing is, therefore, to be qualified as 'purely factual conduct' or, in relation to a decision made by an authority of another Member State, as a preparatory measure.[1716]

Eurodac Hits

A Eurodac hit can conventionally neither be described as administrative conduct with legal effects nor as a binding decision. A hit is the automated consequence of 'purely factual conduct': the collection and comparison of data. The hit itself only achieves a factual result, the knowledge of two data items compared being labelled as the same data. A Eurodac hit is furthermore not a binding decision. Under the old Eurodac Regulation, the authority deciding on a final measure first had to verify the hit's accu-

1712 Case 60/81 *International Business Machines Corporation v Commission of the European Communitie* [1981] ECR 2639, paras 9ff, 11 and 19; Matthias Ruffert, 'Verwaltungsakt' in Hans-Uwe Erichsen and Dirk Ehlers (eds), *Allgemeines Verwaltungsrecht* (De Gruyter 2005), § 20 IV 4 para 69 with references.

1713 cf fn 1708.

1714 Giacinto della Cananea, 'The European Union's Mixed Administrative Proceedings' (2004) 68 Law and Contemporary Problems 197; Edoardo Chiti, 'Chapter 1 - The Administrative Implementation of European Union Law: A Taxonomy and Its Implications' in Herwig C H Hofmann and Alexander H Türk (eds), *Legal Challenges in EU Administrative Law* (Edward Elgar Publishing 2009).

1715 Eliantonio, 'Judicial Review in an Integrated Administration: The Case of "Composite Procedures"' (n 1706) 70.

1716 cf Schneider, 'Information Exchange and Its Problems' (n 1675) 104.

racy.[1717] This provision was not included in the new Eurodac Regulation, where a hit is only checked "where necessary".[1718] As of now, the deciding authority is not bound by what the hit implies. If an asylum seeker first entered the Schengen Area in Italy and then travelled to Germany, the German authority might receive a Eurodac hit but also additional information on the asylum seeker, e.g., that his wife lives in Germany, and therefore will not send them back to Italy.[1719] There is no inevitable link between the hit and the follow-up measure. A hit therefore also constitutes 'purely factual conduct' or a preparatory measure.[1720]

Security Flags

As opposed to the acts just mentioned, a security flag seems to be some sort of a decision. Following the security checks as held in the Screening Regulation, the AMMR, and the Asylum Procedure Regulation,[1721] the fact that a person could pose a threat to internal security is recorded in Eurodac if the person is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in Directive (EU) 2017/541[1722] or in any of the offences referred to in

1717 2016 Eurodac Proposal, Art 26(4). The result of the comparison of fingerprint data carried out pursuant to Article 15 shall be immediately checked in the receiving Member State by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons provided for in this Regulation.

1718 Eurodac Regulation 2024, Art 38(4).

1719 cf Verwaltungsgericht Köln, 11 Januar 2011, 16 L 1913/10A: "Aus dem den vorgelegten Verwaltungsvorgängen zu entnehmenden Umstand (Euordac-Treffer), dass der Antragsteller in Italien im Ort X aufgegriffen wurde, folgt nicht zwingend, dass es sich bei dem nach der Einreise in die Bundesrepublik Deutschland gestellten Asylantrag bereits um einen zweiten – und damit unwirksamen – Asylantrag handelt." ('It does not necessarily follow from the fact (Euordac hit) that the applicant was apprehended in Italy in the town of X that the asylum application submitted after entering the Federal Republic of Germany is already a second - and therefore ineffective - asylum application.').

1720 Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 64.

1721 Eurodac Regulation 2024, Art 17(2)(i), 22(3)(d), 23(3)(e) and 24(3)(f); in conjunction with the Screening Regulation; AMMR and the Asylum Procedure Regulation.

1722 Directive on Combating Terrorism.

Council Framework Decision."[1723,1724] From the Eurodac Regulation itself, it is not clear what information exactly will be stored in Eurodac. It does not provide whether a security flag record is a simple 'tick box' or a free text input system, where a national authority can add information.[1725] One criticism is that this category is not in line with the requirement for clarity and precision, in accordance with the case law of the Court of Justice of the EU.[1726] As was concluded before, it is likely that the first part of the security evaluation, the data comparison, is tick-box style information and the second part requires more information.

The decision that a person could pose a security threat, according to Art. 15 Screening Regulation, seems to be based on 'purely factual conduct'. This is the comparison of data with the ETIAS watchlist or screening rules, with other EU information systems, the Europol and Interpol databases, and with national databases.[1727] Such comparison with a database or list is comparable to the automated comparison that produces a Eurodac hit. It is an automated function that leads to information in the form of a flag. Such information does not inevitably result in a specific action, such as preventing a person from entering the Schengen Area. However, it triggers further investigation and halts the asylum process during that time.[1728] The flag therefore has some legal consequences.

The requirements stated by the Eurodac Regulation require more analysis and assessment of a data subject than mere comparison of data.

1723 EAW Framework Decision - Statements made by certain Member States on the adoption of the Framework Decision.

1724 Eurodac Regulation 2024, Art 17(2)(i) and Recital 8. The list of offences covered by this directive is much shorter than was the case with earlier drafts of the new Eurodac Regulation. However, this limitation is offset by the potentially very broad and defined only in Recital 8 Eurodac Regulation 2024 as "whether the person has displayed behaviour that results in physical harm to other persons that would amount to a criminal offence under national law".

1725 Vavoula, 'Focus on Eurodac: Disentangled from the "Package Approach" but Is It Fit to Fly?' (n 607) 19.

1726 ibid 19; Opinion 1/15 on the Draft Canada-EU PNR Agreement (n 541), paras 155 - 163.

1727 Screening Regulation, Art 11; how the security check according to AMMR, Art 8(4) are conducted is not explained in this regulation.

1728 AMMR, Recital 45: "In order to prevent a person who represents a security risk from being transferred among the Member States, it is necessary to ensure that the Member State where an application is first registered does not apply the responsibility criteria or the benefitting Member State does not apply the relocation procedure where there are reasonable grounds to consider that the person concerned a threat to internal security."

Whether a data subject is considered violent, aunlawfully armed or whether there are clear indicators that they are involved in a crime, seems akin to a decision. Such a decision is legally binding only for the authority responsible for investigating the threat and determining whether it constitutes grounds for exclusion from asylum. This seems similar to an SIS alert, where the alert results from an administrative procedure that involves more than just a simple comparison of information.[1729] However, an SIS alert often has a specific consequence: if an alert for seizure of an object goes off, the object will be seized.[1730] With regard to SIS alerts, it has been assumed that it is of a preparatory nature (and therefore not reviewable).[1731] The ECJ decided, in the case Commission v Kingdom of Spain, with regard to an SIS alert, that both the authorities of the Member State taking the final measure as well as the authorities of the Member State entering the alert into the system are obliged to verify the conditions of the follow-up action. In that case, this was the refusal of entry into the Schengen Area.[1732] An SIS alert cannot be considered a binding decision. This cannot be assumed for security flags, either. The flag alone does not change the data subject's legal position. A security flag must therefore be qualified as 'purely factual conduct' or a preparatory act.

Conclusions

Information sharing, Eurodac hits, and security flags must be classified either as 'purely factual conduct' (Realakte) or, when they ultimately lead to a final decision, as preparatory measures for that decision. The key questions, therefore, are: can these acts be subject to review at all? And, if so, can they be reviewed when carried out by another Member State?

1729 cf SIS II Regulation.

1730 ibid, Art 38; in parts also SIS II Decision.

1731 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553) 542.

1732 *Commission of the European Communities v Kingdom of Spain* (n 1687), paras 52, 55, and 59; Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684) 147 - 164.

bbb) *Reviewing Preparatory Measures*

Art. 47 CFR does not generally require judicial review of preparatory decisions.[1733] Moreover, the EU system of judicial review entails two characteristics that are relevant obstacles to a comprehensive review of factual conduct potentially affecting individual rights.[1734] First, EU law does not explicitly provide an action for a declaratory order, while the annulment action under Art. 263 TFEU requires a reviewable act. The second obstacle is that the EU system of judicial review is regulated by Treaties. Thus, the CJEU is reluctant to expand its powers through case law and even tends to restrict options for legislative expansion in some cases.[1735] This is different from Art. 13 ECHR, which covers the entire spectrum of non-binding sovereign acts.[1736] The ECtHR's position on reviewing preparatory measures will be discussed in the next section, along with the question whether 'purely factual conduct' can be reviewed. As it is not required by Art. 47 CFR preparatory measures may be incapable of being autonomously challenged at the national level, especially when they are considered incapable of directly affecting the applicant's legal sphere. This has been argued for preparatory measures in composite procedures.[1737] It might, however, be possible to challenge preparatory measures with the final decision. The ECJ, even though it stated in its Samba Diouf case that there need not be an appeal against a decision made in preparation of the final decision – such as the decision to conduct an asylum application in an accelerated procedure – took that stance only provided that the legality of the final decision may be subject of a "thorough review".[1738] It seems that a review of preparatory measures may be possible, when the final decision is thoroughly reviewed.

1733 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.138; *Brahim Samba Diouf v Ministre du Travail, de l'Emploi et de l'Immigration* (n 1613), paras 55 - 56.

1734 Schneider, 'Information Exchange and Its Problems' (n 1675) 104.

1735 ibid 104ff.

1736 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 213 ff with references; e.g., *Chahal and Others v the United Kingdom* (n 1308), para. 154; ECtHR, 'Guide on Article 13 of the European Convention on Human Rights: Right to an Effective Remedy' (n 827).

1737 Eliantonio, 'Judicial Review in an Integrated Administration: The Case of "Composite Procedures"' (n 1706) 82, based on research in Italy and Germany.

1738 *Brahim Samba Diouf v Ministre du Travail, de l'Emploi et de l'Immigration* (n 1613), para 56; Similarly, in the already mentioned *Hans-Martin Tillack v Commission of the European Communities* (n 1619), the CJEU held that although the transfer of data itself could not be considered a reviewable act, in response to

With regard to composite procedures, the ECJ stated in the Berlioz case, as already mentioned, that the right to an effective judicial remedy under Art. 47 CFR requires that one national administration must be able to review another Member State administration's decision.[1739] The case did not refer to preparatory decisions but an information order against a subject of a pecuniary fine, which is a binding decision that has legal effects.[1740] In its

---

the suggestion that this conclusion may deprive the applicant of effective judicial protection, it did state that the applicant had the opportunity to bring an action before the national court and ask it to request a preliminary reference ruling from the CJEU.

1739 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530), para 66ff; It should be added here, that there are, with regard to Eurodac, other more rare constellations that would lead to another result. First, where the EU procedural rules establish that the final decision is taken by a national authority, in cases where an EU institution or body has given input into the decision-making procedure or the EU institution is bound by a national act and has "only limited or no discretion", *Silvio Berlusconi, Fininvest v IVASS* (n 1559), para 45); it is for national courts to ensure effective judicial remedies of the act, "even if the national rules of procedure do not so provide", *Silvio Berlusconi, Fininvest v IVASS* (n 1559), para 46; This constellation might occur, where Europol has provided input into a decision, for example by declaring a person to be a security threat. In this case a preliminary reference under TFEU, Art 267 would be the means to ensure incidental control of the validity or interpretation of preparatory acts of EU institutions, as it is it is for national courts to ensure effective judicial remedies of the act (Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), para 47.140ff.; referencing *Oleificio Borelli v. Commission of the European Communities* (n 1529), paras 9 - 13; as well as Case C-269/99 *Carl Kühne GmbH & Co KG and Others v Jütro Konservenfabrik GmbH & Co KG* [2001] ECR I-9517, para 58; Case C-343/07 *Bavaria NV, Bavaria Italia s.r.l v Bayerischer Brauerbund eV* [2009] OJ C 205/3, para 57); A second possible constellation is that EU law states that an EU body, office or agency, such as eu-LISA has exclusive decision-making power. It then falls, according to the CJEU, "to the EU Courts, by virtue of their exclusive jurisdiction to review the legality of EU acts on the basis of TFEU, Art 263, to rule on the legality of the final decision adopted by the EU body, office or agency concerned and to examine, in order to ensure effective judicial protection of the persons concerned, any defects vitiating the preparatory acts or the proposals of the national authorities that would be such as to affect the validity of that final decision" (Case C-414/18 *Iccrea Banca SpA Istituto Centrale del Credito Cooperativo v Banca d'Italia* [2019] OJ C 36/7, para 39; referring to *Silvio Berlusconi, Fininvest v IVASS* (n 1559), para 44.

1740 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530). The Berlioz case did not address the right to judicial review in the sole presence of an information order issued without the application of a pecuniary fine. In that case, it might have been arguable that the order does not aim at a legal effect, but merely a factual result and therefore might have been considered 'purely factual conduct'.

Oleificio Borelli case, the ECJ held that a national measure that prevented legal action from being taken against a mere administrative preparatory act would be in violation of the right of access to justice.[1741] Eliantonio has suggested that if this case law is taken seriously, it should be possible to review an SIS alert.[1742] Nevertheless, no case in front of an EU court, so far, has specifically addressed the issues of a preparatory decision of another Member State. In the Forabosco case, the French Coucil of State reviewed an SIS alert by Germany and thus a preparatory decision.[1743]

Mazzotti and Eliantonio have suggested that transnational judicial review should be possible in the context of claims against the final act, when preparatory measures are not challengeable.[1744] This means that judicial bodies with full review power could examine preparatory measures in a claim against the final decision. In horizontal cases, the court reviewing the final formal decision of an authority from its own jurisdiction may – in general – also review factual input, for example, based on information exchange from another Member State. Problems arise when reviewing the reviewing standard by a foreign country, or when it may be difficult to identify the source of information for a final decision.[1745] Decision-making on the basis of composite procedures with the help of information systems results in a separation between decision-making and the preparation thereof. Scholars have brought forward other solutions to this problem than revision of foreign preparatory measures.[1746] None, so far, has been

1741 *Oleificio Borelli v Commission of the European Communities* (n 1529).

1742 Eliantonio, 'Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?' (n 1553).

1743 Conseil d'État, 190384 (n 1693). The French Conseil d'Etat did not undertake a legal qualification of the SIS alert in its decision. It is thus unclear whether it thought of the alert as a preparatory decision and would apply its decision law to other preparatory measures, such as a 'hit'.

1744 Mazzotti and Eliantonio, 'Transnational Judicial Review in Horizontal Composite Procedures: Berlioz, Donnellan, and the Constitutional Law of the Union' (n 1704) 69: "this solution, moreover, finds a powerful conceptual justification in the notion that all judges in all Member States are to be regarded as "EU courts of general jurisdiction", or as *juges de droit commun*. If each and every national court is to be regarded as equally called upon in applying EU law, there seems to be no reason for administrative acts meant to execute such law not to be reviewed in the light of the applicable norms for the mere reason that they emanate from authorities of another Member States."

1745 cf Schneider, 'Information Exchange and Its Problems' (n 1675) 108.

1746 A whole raft of other possible adjustments has been presented in the past by Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684), to solve the issue that decision-making on the basis

implemented. The only proposal regarding migration information systems that has been discussed and has, at least partially, come to fruition is the establishment of an EU body to manage information systems,[1747] now embodied in eu-LISA. However, contrary to initial expectations, eu-LISA lacks "decision-making, and to a certain degree, mediation powers and its acts [are not] subject to judicial review on the EU level" [1748], at least in many cases. This could change if the web portal[1749] hosted by eu-LISA were developed into a comprehensive complaints mechanism for EU information systems.[1750]

At present, Member States generally do not review preparatory measures. Under European law, they are not required to review preparatory measures taken by other Member States when issuing their own final decision. In practice, they sometimes do, as illustrated in the Forabosco case, but there is no general rule or expectation that they must.

---

of composite procedures with the help of information networks results in a separation between decision-making and the preparation thereof; First, the enlargement of the notion of 'reviewable acts' under TFEU, Art 263, to include factual conduct or preparatory acts, or such acts could be reviewed under Art. 263 TFEU based on the notion of 'tacit decision'; Second, based on the Borelli case, national courts could treat preparatory measures or factual conduct "as admissible even where domestic rules do not provide for such a case", *Oleificio Borelli v Commission of the European Communities* (n 1529), para 13. Third, as the French Council State did in Forabosco by reviewing the lawfulness of a German Schengen alert on the basis of the Schengen Convention, national courts could find solutions on the basis of a conflict of laws approach. Fourth, allowing courts of Member States to obtain a preliminary ruling from courts of other Member States, or to allow for the CJEU to refer questions to national courts as to the application of national law in composite procedures. And finally, based on a principle of subrogation each network members' jurisdiction could be made competent to rule on tort claims brought against actions of any of the network members.

1747 Tidghi, 'Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks' (n 1684) 163.

1748 ibid 163.

1749 Interoperability Regulation - Judicial Cooperation, Art 48.

1750 Some version of this was suggested by FRA, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications', (n 71) 51. Although in this vision, the web-portal would only handle the requests EU-wide and not alter the Member States responsibility.

ccc) *Reviewing 'Purely Factual Conduct'*

Under the European Charter of Fundamental Rights

The CJEU does not use the concept of 'purely factual conduct'. Art. 47 CFR grants the right to an effective remedy to any person "whose rights and freedoms guaranteed by the law of the Union have been violated". If an act of the Union affects the interests of a person, this is not in itself sufficient to give that person the right to an effective remedy; rather, the interest affected must be recognised as a legally defensible position, meaning the person must have a subjective right.[1751] If a subjective (or individual) right is violated, then a remedy must be available.[1752] Certain subjective rights define factual conduct with sufficient precision so that particular acts or omissions can amount to a violation of the subjective right within the meaning of Art. 47 CFR. An example of this is Art. 8 CFR. It stipulates that data processing may only be carried out under certain conditions.[1753] The ECJ decided that "[...] the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Art. 8 of the Convention. To establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive

1751 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 174ff; cf also Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.68ff.

1752 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 174ff; Case C-104/13 *Olainfarm AS v Latvijas Republikas Veselības ministrija, Zāļu valsts aģentūra* [2014] OJ C 439/3; Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.72.

1753 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 174ff. Rademacher distinguishes between actions that are prohibited as such (e.g. Art. 4 CFR prohibition of inhuman or degrading treatment) and actions that are prohibited on the basis of a reaction-related perspective, which, according to him, includes data processing. In addition, Rademacher also examines subjective rights, which do not specifically describe and prohibit specific acts, but rather designate certain forms of behaviour by individuals as protected vis-à-vis the state. What is usually missing in these subjective rights is a concrete description of the specific conduct against which they protect individuals. Rademacher argues that these rights are not only protected if they are affected by a legal mechanism. However, this is unclear in the practice of the CJEU; As an example, Case 249/81 *Commission of the European Communities v Ireland* [1982] ECR I-4005, is discussed by Rademacher, in which it was heard whether an advertising campaign that called to "Buy Irish!" violated the fundamental freedom of free movement of goods.

character or whether the persons concerned have been inconvenienced in any way".[1754] The mere act of sharing data with another Member State can, it seems, be subjected to review insofar as it concerns whether the legal conditions governing such data transmission were fulfilled.

Eurodac hits and security flags constitute the results of the processing of personal data. Since such data are protected under Art. 8 CFR, they are in principle open to review whether the conditions for their processing have been fulfilled. However, in Eurodac cases, the central questions arising in relation to hits and flags rarely concern whether the requirements for data processing leading to the production of a hit or flag were met. Instead, they focus on whether the results are appropriate and can be challenged, either in connection with or independently of a final decision. The subjective right, in this case, might derive from the right to good administration, codified in Art. 41 CFR. As a general principle of EU law, this binds not only EU institutions and bodies but also Member States in all procedures.[1755] It is not clear whether this would lead to a remedy against 'purely factual conduct' by an administration. Another provision from which a subjective right might be derived is Art. 5(1)(d) GDPR, stipulating that personal data have to be "accurate and, where necessary, kept up to date". This request is specific and applies to all data under the GDPR. It is argued here that Art. 5(1)(d) GDPR establishes a subjective right. Accordingly, if a data subject asserts that a Eurodac hit or a security flag is inaccurate, they must be afforded access to an effective remedy within the meaning of Art. 47 CFR in order to challenge such acts.

With regard to composite procedures, the same observations apply as in the preceding section. To date, no EU court has addressed the problem of 'purely factual conduct' carried out by another Member State, not least because EU courts do not employ the concept of 'purely factual conduct' in their jurisprudence.

1754 *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* (n 1226), para 74ff; referencing *Amann v Switzerland* (n 1227), para 70.

1755 Craig, 'Article 41 - Right to Good Administration' (n 880), para 41: "However, Article 41 on its face is framed in terms of EU institutions, bodies, offices and agencies, and there is authority for this literal interpretation. The position taken by the CJEU is more nuanced. The Court recognises that Article 41 refers only to EU institutions, bodies and agencies, and thus cannot in itself be relied on as against a Member State, but that the right to good administration constitutes a general principle of EU law, which includes, inter alia, the provision of reasons and the right to a hearing, and this binds the Member States when they act in the scope of EU law."

Under the European Convention on Human Rights

The ECtHR adopts a position that differs slightly from that of the CJEU. As noted above, Art. 13 ECHR covers the full range of non-binding sovereign acts.[1756] Accordingly, an applicant before the ECtHR need not demonstrate that they hold a legal position amounting to a subjective right. The collection, storage, and disclosure of personal data each constitute an interference with Art. 8 ECHR.[1757] Data sharing is a form of disclosure and therefore interferes with Art. 8 ECHR and may be challenged. The ECtHR has further held that an individual must have the possibility to contest the storage of data or to refute the accuracy of stored information, including where such data are retained for security purposes.[1758] A security flag constitutes personal data,[1759] and its retention accordingly interferes with Art. 8 ECHR. The same applies to a Eurodac hit.[1760]

In principle, Member States must provide effective remedies against data sharing, Eurodac hits, and security flags where these qualify as 'purely factual conduct'. The question of how such remedies must be structured, and whether compensatory or indirect judicial remedies are sufficient, has been addressed above.

1756 Rademacher, *Realakte im Rechtsschutzsystem der Europäischen Union* (n 1515) 213ff with references.

1757 *Torsten Leander v Sweden* (n 523), para 48.

1758 *Rotaru v Romania* (n 865), para 72.

1759 A flag is, in part, the result of data-comparison of personal data by the data subjects with data in other databases (e.g., SIS, Europol) or risk lists (e.g. ETIAS watchlist) and as such comparable to a hit, which is also considered personal data (cf *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* (n 1226)); Other information that is included in an assessment of a person being a security threat is the evaluation of personal data of the data subject by an authority, that may be comparable to an evaluation by a teacher, such as in *Peter Nowak v Data Protection Commissioner* (n 1033), which is also considered to be personal data.

1760 A hit, indicating that personal data of a person is already stored in the Eurodac information system constitutes personal data in the sense of GDPR, Art 4(1); according to Art. 29 WP, 'Opinion on Commission Proposals for Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as Well as Police and Judicial Cooperation, Asylum and Migration' (n 683) 13: "The so-called "hit-flag" indicating that data on a person are stored in the CIR, constitutes personal data." A hit indicating that data is stored in Eurodac must, accordingly, also be considered personal data.

b) *Mutual Trust*

The principle of mutual trust obliges Member States to presume – save in exceptional circumstances – that all other Member States comply with EU law, and in particular with the fundamental rights guaranteed by EU law.[1761] At first sight, this presumption appears to exclude the possibility of reviewing an act undertaken by another Member State. This section therefore examines the circumstances in which the principle of mutual trust may be displaced, thereby enabling the review of another Member State's act. The second part of the section addresses additional difficulties arising from the fact that certain acts – most notably Eurodac hits – are the outcome of technical and automated processes. These features raise particular questions regarding the feasibility and scope of review.

aa) Conditions for Mutual Trust – and its Loss

Mutual trust is one of the cornerstones of judicial cooperation in the EU.[1762] It is a concept without a clear normative foundation. Its content and meaning in the present context must, and can, be derived from the case law of the CJEU, as will be demonstrated below. The system of inter-state cooperation established by the Dublin III and Eurodac Regulations is based on a structure of negative mutual recognition. Mutual recognition creates extraterritoriality[1763] and presupposes mutual trust:[1764] within a borderless Area of Freedom, Security and Justice, mutual recognition is intended to ensure that a decision of an authority in one Member State can be enforced beyond its territorial legal borders and across this area, speedily and with a minimum of formality.[1765] The principle of mutual trust implies that

1761 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others*, Opinion of AG Kokott (n 705), para 155.

1762 'Challenges Related to Mutual Trust Concerns Raised in Appeals within the Dublin III Procedure' (European Union Agency for Asylum 2023) 2.

1763 Kalypso Nicolaïdis, 'Trusting the Poles? Constructing Europe through Mutual Recognition' (2007) 14 Journal of European Public Policy 682.

1764 Valsamis Mitsilegas, 'The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU' (2006) 43 Common Market Law Review 1277.

1765 ibid, 'Solidarity and Trust in the Common European Asylum System' (2014) 2 Comparative Migration Studies 181, 190.

Member States establish mutual trust in the quality and lawfulness of each other's laws and practices and act accordingly.[1766]

Trust between Member States is a core principle underpinning the operation of Eurodac. When a hit occurs, administrative authorities generally proceed on the presumption that, at the time the Eurodac record was created, the individual concerned either lodged an application for international protection or was apprehended as an irregular migrant. Responsibility for examining the asylum claim is therefore assumed to lie with another Member State. As Vavoula has correctly pointed out, this presumption is based on the existence of a technology-based trust that operates on two levels.[1767] First, there exists interstate trust, among national administrations, that the fingerprints are lawfully and carefully collected and transmitted, the rights of the fingerprinted third-country nationals are safeguarded, and the record entered in Eurodac is accurate, of high quality, up-to-date, and compliant with the rights to dignity,[1768] respect for private life,[1769] and personal data protection.[1770,1771] In addition, Eurodac exemplifies trust among Member States in overseeing the external borders of the EU by eagerly fingerprinting irregular entrants. Additionally, interstate trust in procedures is facilitated by trust in technology and the belief that biometric identifiers, including fingerprints, along with their centralised storage, are trustworthy advents.[1772]

Mutual trust should and will remain a core principle once interoperability becomes fully operational. The same assumptions mentioned above must continue to apply, even if additional authorities and information systems are linked to Eurodac, thereby expanding the scope of the system. However, it is expected that interoperability will "redraw known frontiers" with regard to the EU's commitment to the protection of fundamental rights and the

1766 cf Opinion 2/13 Concerning Accession to the ECHR [2014], Opinion of the Full Court.

1767 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 398.

1768 CFR, Art 1.

1769 ibid, Art 7.

1770 ibid, Art 8.

1771 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 398; cf also Mitsilegas, 'Solidarity and Trust in the Common European Asylum System' (n 1765).

1772 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 398.

constitutional principle of mutual trust between the Member States.[1773] The need to reconcile mutual trust with the limits derived from fundamental rights is one of the EU's most pressing contemporary constitutional challenges.[1774] Mutual trust remains an ambiguous and multifaceted concept.[1775]

The concept of mutual trust, which originates from internal market law and is nowadays applied in manifold ways in EU law,[1776] translates predominantly as a legal requirement for Member States to generally presume adherence to EU fundamental rights by their peers.[1777] The ECJ has expressed this in clear terms in its Opinion 2/13.[1778] The Court specified in a later judgment that "the principle of mutual trust requires, particularly as regards the area of freedom, security and justice, each of those States,

1773 Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 66.

1774 ibid 66; cf Mattias Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (2019) 15 European Constitutional Law Review 17; cf Auke Willems, 'The Court of Justice of the European Union's Mutual Trust Journey in EU Criminal Law: From a Presumption to (Room for) Rebuttal' (2019) 20 German Law Journal 468; cf Koen Lenaerts, 'La vie après l'avis: Exploring the Principle of Mutual (yet Not Blind) Trust' (2017) 54 Common Market Law Review 805; cf Stefano Montaldo, 'On a Collision Course! Mutual Recognition, Mutual Trust and the Protection of Fundamental Rights in the Recent Case-Law of the Court of Justice' (2016) 1 European Papers - A Journal on Law and Integration 965; cf Valsamis Mitsilegas, '13 - Mutual Recognition and Fundamental Rights in EU Criminal Law' in Sara Iglesias Sánchez and Maribel González Pascual (eds), *Fundamental Rights in the EU Area of Freedom, Security and Justice* (Cambridge University Press 2021).

1775 Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 20.

1776 cf *Slowakische Republik v Achmea BV* (n 1531), paras 34 and 58; ppecifically regarding the principle of mutual recognition which is derived from the principle of mutual trust: Michael Schwarz, *Grundlinien der Anerkennung im Raum der Freiheit, der Sicherheit und des Rechts* (Mohr Siebeck 2016) 151ff and 205ff.

1777 Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 21; A second kind of trust is that a Member State 'may not demand a higher level of national protection of fundamental rights from another Member State than that provided by EU law', cf Opinion 2/13 Concerning Accession to the ECHR (n 1766), para 192; in line with Case C-399/11 *Stefano Melloni v Ministerio Fiscal* [2013] OJ C 114/12, para 60, national authorities and courts are, of course, still free to require higher standards of protection provided that neither the level of protection under EU law nor the principles of primacy, unity, and effectiveness of EU law are thereby compromised. However, national authorities and courts cannot be obliged to do so by their peers.

1778 Opinion 2/13 Concerning Accession to the ECHR (n 1766), para 191.

save in exceptional circumstances, to consider all the other Member States to be complying with EU law and particularly with the fundamental rights recognised by EU law."[1779] The principle hence establishes a horizontal presumption of Member State compliance with EU fundamental rights – a presumption which can only be rebutted in exceptional circumstances.[1780] The CJEU has regularly been called upon to determine the conditions for that 'point of rebuttal'.[1781] This has occurred prominently in cases involving intra-European transfers of persons. However, as Advocate General Laila Medina stated, EU law does not provide for the principle of mutual recognition with regard to positive decisions granting refugee status.[1782] The CJEU confirmed this position, noting that EU law on international protection does not, as it currently stands, impose an express obligation on the Member State to recognise automatically decisions granting refugee status adopted by another Member State.[1783] Member States are, however, free to do so. In the light of the principle of sincere cooperation set out in Art. 4(3) TEU, the competent authority of the Member State called upon to decide on the new application must, as soon as possible, initiate an exchange of information with the competent authority of the Member State that previously granted refugee status to the same applicant.[1784] The ECJ ruled that when the competent authority of a Member State cannot reject an application for international protection as inadmissible, it must take further action. This situation arises when another Member State has already granted protection to the applicant, and there is a serious risk that the

1779 *Minister for Justice and Equality v LM* (n 186), para 36.

1780 Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 21.

1781 cf Georgios Anagnostaras, 'The Common European Asylum System: Balancing Mutual Trust Against Fundamental Rights Protection' (2020) 21 German Law Journal 1180; Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 22.

1782 Case C-753/22 *QY v Bundesrepublik Deutschland* [2022] OJ C 104/14 (Effect of a decision granting refugee status); Case C-753/22 *QY v Bundesrepublik Deutschland* [2024], Opinion of AG Medina, paras 51 and 75; with regard to mutual recognition of negative asylum decisions, there is some debate about what counts as such a recognition and what not. For this discussion see Joined Cases C-297/17, C-318/17, C-319/17 and C-438/17 *Bashar Ibrahim and Others v Bundesrepublik Deutschland and Bundesrepublik Deutschland v Taus Magamadov* [2019] OJ C 187/11, para 58; *Joined Cases C-123/23 and C-202/23 Khan Yunis and Baabda* [2024] Opinion of AG Nicholas Emiliou, para 76ff.

1783 *QY v Bundesrepublik Deutschland* (n 1782), para 56.

1784 ibid, para 78.

applicant will face inhuman or degrading treatment in that other Member State (as outlined in Art. 4 CFR). In such cases, the authority must conduct a new, individual, and comprehensive examination of the application in a new international protection procedure. In the course of this examination, the authority must take into account the decision of the other Member State to grant international protection to the applicant, along with the factors that informed that decision.[1785]

Only very serious violations of fundamental freedoms seem to undermine the principle of mutual trust. Art. 43(1)(b) AMMR envisages circumstances arising after a transfer decision that may affect the proper application of the AMMR and give rise to an appeal against the transfer. A more critical provision, however, is Art. 43(1)(a) AMMR, which provides that an individual must not be transferred if there is a real risk of inhuman or degrading treatment within the meaning of Art.4 CFR. This principle was highlighted in the ECJ case Abubacarr Jawo v Bundesrepublik, which addressed the living conditions for asylum seekers in Italy.[1786] The Court stated that a tribunal must assess the standard of protection for fundamental rights in another state when the individual provides evidence of a risk of violating Art. 4 CFR and, *mutatis mutandis*, Art. 3(2) Dublin III Regulation (which has been replaced by Art. 43(1)(a) AMMR).[1787] In its judgment in the case Tarakhel v Switzerland, the ECtHR took into consideration the specific needs of certain categories of asylum seekers, *in casu* families and minors.[1788] Ather cases demonstrated that deficiencies leading to the breakdown of mutual trust can also be procedural in nature. In the cases M.S.S v Belgium and Greece[1789] and S.H. v Malta,[1790] the ECtHR held that mutual recognition also may be refused where access to the asylum system

1785 ibid, para 80.
1786 *Abubacarr Jawo v Bundesrepublik Deutschland* (n 1432).
1787 ibid, para 90.
1788 *Tarakhel v Switzerland* (n 1468) para 115; Further landmark cases that concerned the ban on Dublin transfers to a number of other Member States because of systemic deficiencies are: *M.S.S v Belgium and Greece* (n 1468) and *N. S. v Secretary of State for the Home Department and M E and Others v Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform* (n 1436); Other cases particularly considered detention facilities, such as Case C-528/15 *Policie ČR,Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor* [2017] OJ C 151/8 and *Feilazoo v Malta* App no 6865/19 (ECtHR, 11 March 2021).
1789 *M.S.S v Belgium and Greece* (n 1468), para 286ff.
1790 *S.H. v Malta* App no 37241/21 (ECtHR, 20 December 2022).

or an effective remedy are lacking, leading to a breach of Art. 3 ECHR in conjunction with Art. 13 ECHR. Another ground for setting aside mutual trust is the risk of pushbacks or indirect refoulement. This was affirmed in, among other cases, the landmark ruling of M.S.S v Belgium and Greece.[1791]

In the case N.S. and others, the ECJ initially suggested that the existence of "systemic flaws in the asylum procedure and reception conditions for asylum applicants", resulting in inhuman or degrading treatment, would render a transfer of asylum seekers to the state of destination illegal in and of itself, without the need to carry out an additional individualised risk assessment.[1792] While the Court did not further clarify in N.S. and others whether prohibitions on transfers are also admissible below the threshold of systemic deficiencies, the Grand Chamber subsequently denied such a possibility in its case Abdullahi.[1793] In CK and others clarified that the existence of systemic flaws in a Member State does not need to be established in every case. It held that an individualised risk assessment may be sufficient.[1794] In that case, the real risk for the applicant emanated, according to the Court, from the transfer itself rather than from the human rights situation in the other country.[1795] Most recently, Advocate General Kokott determined: when reviewing a transfer decision under Art. 27 Dublin III

1791 *M.S.S v Belgium and Greece* (n 1468); cf also *Sharifi and Others v Italy and Greece* App no 16643/09 (ECtHR, 21 October 2014).

1792 *N. S. v Secretary of State for the Home Department and M. E. and Others v Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform* (n 1436), para 86; for a more detailed description of the shift of the Court see Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774), in particular 24f.

1793 *Shamso Abdullahi v Bundesasylamt* (n 1433), paras 52ff and 60.

1794 Case C-578/16 PPU *C.K., H.F., A.S. v Republika Slovenija* [2017] OJ C 112/11, paras 65 and 92ff; cf EUAA, 'Challenges Related to Mutual Trust Concerns Raised in Appeals within the Dublin III Procedure' (n 1762) 4; For an examination in more detail see Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 24.

1795 *C.K., H.F., A.S. v Republika Slovenija* (n 1794), paras 90 and 95: "Finally, that interpretation fully respects the principle of mutual trust since, far from affecting the existence of a presumption that fundamental rights are respected in each Member State, it ensures that the exceptional situations referred to in the present judgment are duly taken into account by the Member States. Moreover, if a Member State were to proceed with the transfer of an asylum seeker in such situations, the resulting inhuman and degrading treatment would not be attributable, directly or indirectly, to the authorities of the Member State responsible, but to the first Member State alone."

Regulation (replaced by Art. 43(1) AMMR), it must be assumed that a breach of mutual trust is an exception. Examining whether the principle of non-refoulement or other fundamental rights guarantees may be infringed by another Member State is warranted only when there is evidence of significant deficiencies in that Member State. These deficiencies must reach a particularly high level of severity and possess a general, systemic nature.[1796] The ECJ confirmed this opinion in its judgment on the case.[1797]

Scholars have nevertheless pointed out that limits to the principle of mutual trust can be set by fundamental rights that are not protected in absolute terms, unlike Art. 4 CFR, to the extent that there is a real risk to their essence.[1798] In the case LM,[1799] the ECJ ruled that transfers of

1796 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), paras 156 and 160; cf also ECRE, 'CJEU: AG Opinion Regarding Member State's Obligations on the Right to Information, a Personal Interview and the Principle of Non-Refoulement' (*elenaforum.org*, 20 April 2023) <https://elenaforum.org/cjeu-ag-opinion-regarding-member-states-obligations-on-the-right-to-information-a-personal-interview-and-the-principle-of-non-refoulement/>.

1797 *Ministero dell'Interno, Dipartimento per le Libertà civili e l'Immigrazione – Unità Dublino and Others v CZA and Others* (n 714), paras 142 and 152; there is also some case law on the national level dealing with the issue of mutual trust. E.g., The Court of The Hague annulled a Dublin transfer to Belgium because the burden of proof on the applicability of the interstate principle of mutual trust shifted to the national authorities in view of ECtHR interim measures ordered to the government of Belgium, Rechtbank den Haag, 20 februari 2023, NL23.382 (*verzoeker / de Staatssecretaris van Justitie en Veiligheid)*; cf also Rechtbank den Haag, 4 oktober 2021, NL21.4376 *(eiser, geboren 1994, van Soedanese nationaliteit / de staatssecretaris van Justitie en Veiligheid, beveiligdder*).

1798 Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 18; Cecilia Riczallah, 'The Principle of Mutual Trust in EU Law in the Face of a Crisis of Values' (*The EAPIL blog*, 22 February 2021) <https://eapil.org/2021/02/22/the-principle-of-mutual-trust-in-eu-law-in-the-face-of-a-crisis-of-values/>.

1799 *Minister for Justice and Equality v LM* (n 186). The case is also known as Celmer, due to the non-anonymised names of the relevant parties in the Irish main proceeding; According to Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 26, the ground-breaking nature of LM lies in its explicit assignment of the guarantee of judicial independence to the essence of the basic right to a fair trial. The European Court of Justice derives from Article 47(2) CFR a fundamental right to an independent tribunal and also designates it as such a breach of this fundamental right to an independent tribunal entails a breach of the essence of a person's fundamental right to a fair trial. Although the Court does not state this explicitly, one can assume that the fundamental right to an independent tribunal,

individuals from one EU Member State to another are prohibited, should a lack of judicial independence threaten the essence of the right to a fair trial. With that, it was argued, the ECJ acknowledged that mutual trust can be refused because of a real risk to the essence of a fundamental right.[1800] Scholars have argued the same with regard to cases in other areas of law, such as the enforcement of judgments in civil and commercial matters.[1801]

Furthermore, other cases, while not explicitly addressing the principle of mutual trust, also suggest more boundaries to its application. In Commission v Kingdom of Spain, the ECJ held that an authority that has not issued an SIS alert cannot rely on it but must verify whether the presence of a data subject constitutes a genuine, present, and sufficiently serious threat, before taking action. Also, based on the principle of genuine cooperation, the authority that issued an SIS alert has to "make supplementary information available" to the consulting Member State.[1802] More recently, in the case E,[1803] the ECJ advanced this point further. The Court held that individuals affected by a return decision accompanied by an SIS alert may, when challenging such a decision, invoke the obligations of the authorities in the state issuing the alert. These authorities are required to consult with the authorities of other Member States to obtain all relevant information necessary for making a decision.[1804]

---

being part of the essence of Art. 47(2) CFR, is framed much more narrowly than Art. 47(2) CFR in its entirety.

1800 Wendel, 'Mutual Trust, Essence and Federalism – Between Consolidating and Fragmenting the Area of Freedom, Security and Justice after *LM*' (n 1774) 18.

1801 Riczallah, 'The Principle of Mutual Trust in EU Law in the Face of a Crisis of Values' (n 1798), pointed out that in the Krombach case, mutual trust was refused because the defendant has suffered "a manifest breach of his right to defend himself before the court of origin" (Case C-7/98 *Dieter Krombach v André Bamberski* [2000] ECR I-1935, para 44); in Case C-619/10 *Trade Agency Ltd v Seramico Investments Ltd* [2012] OJ C 331/3, para 62, the CJEU stressed that only where the defendant's right to a fair trial is "manifestly" breached, leading to the "impossibility of bringing an appropriate and effective appeal" against the judgment in the issuing state, mutual trust is excluded.

1802 *Commission of the European Communities v Kingdom of Spain* (n 1687), para 56.

1803 Case C-240/17 - *E* [2018] OJ C 83/7, paras 56 - 60.

1804 ibid, para 57; according to Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55) 67, the E ruling's significance in interoperability as a whole is that the CJEU explicitly recognises that adequate cooperation between authorities linked by an information system, being essential to ensure that all relevant information is circulated and carefully assessed, must be considered justiciable in view of its "tangible effects on the rights and interests of individuals".

In summary, the case law of the ECtHR and in particular the CJEU is not completely coherent. It cannot be conclusively clarified in which cases the principle of mutual trust precludes a review of an act of another Member State. Illustrative of these legal uncertainties are the numerous preliminary references submitted to the CJEU.[1805] At the same time, transforming Member States into watchdogs of their peers[1806] is not an entirely unproblematic endeavour. For instance, a German judge should not be obliged to acts as a general supervisory authority over Hungarian counterparts, or vice versa.[1807] Nor, however, should the Member States assist each other in committing violations of human rights.[1808] Eurodac is simultaneously a result of and a tool for fostering interstate trust in the Schengen Area. In the current context, two scenarios that can render mutual trust non-applicable should be distinguished: human flaws and technical flaws. A review of an act by another Member State seems possible, if the data collection process is systemically flawed, such as in the case of the consistent false registration of the age of minors, the non-registration of asylum claims for groups of persons, the systemic flagging of certain groups of data subjects as security threats, etc. As seen above, a review may even be possible in individual cases, if there is a risk of a violation of Art. 4 CFR or Art. 3 ECHR, or if the essence of other fundamental rights is infringed. What, however, if not

1805 Asylum Information Database, 'The Implementation of the Dublin III Regulation in 2022' (ECRE 2023) 19: "[...] including three queries from the Netherlands since 2021 regarding the principle of inter-state trust in the context of Dublin returns" with reference to *X v Staatssecretaris van Justitie en Veiligheid* (n 1426); see for more details EUAA, 'NL: The Court of the Hague Referred Questions for Preliminary Ruling on the Application of the Principle of Mutual Trust in the Dublin Procedure' (*caselaw.euaa.europa.eu*, 15 June 2022) <https://caselaw.euaa.europa.eu/pages/viewcaselaw.aspx?CaseLawID=2591>. It should be noted that the previous two preliminary references submitted by Dutch courts were later withdrawn before the CJEU issued a ruling. See the initial preliminary references Case C-208/22 *F v Staatssecretaris van Justitie en Veiligheid* [2022] OJ C 257/22 and Case C-614/21 *G v Staatssecretaris van Justitie en Veiligheid* [2021] OJ C 2/23.

1806 Iris Canor, 'My Brother's Keeper? Horizontal Solange: "An Ever Closer Distrust Among the Peoples of Europe"' (2013) 50 Common Market Law Review 383, 383ff.

1807 Jan Bergman, 'Das Dublin-Asylsystem' [2015] 35(3) Zeitschrift für Ausländerrecht und Ausländerpolitik (ZAR) 81 and 86.

1808 In that sense, cf also Mathias Hong, 'Human Dignity, Identity Review of the European Arrest Warrant and the Court of Justice as a Listener in the Dialogue of Courts: Solange-III and Aranyosi: BVerfG 15 December 2015, 2 BvR 2735/14, Solange III, and ECJ (Grand Chamber) 5 April 2016, Joined Cases C-404/15 and C-659/15 PPU, Aranyosi and Căldăraru' (2016) 12 European Constitutional Law Review 549, para 92.

a human mistake led to the error in Eurodac data?[1809] Trust in the accuracy of Eurodac data extends beyond mutual trust among Member States; it also encompasses trust in the technical infrastructure of EU information systems. Eurodac is managed by eu-LISA and relies both on the proper implementation by Member States and on the reliability of its technical tools. The question therefore is: can these tools always be trusted?

bb) Trust in the Age of Automated Administrative Systems

Undoubtedly, biometric identifiers have been heralded as revolutionary tools that present a series of attractive characteristics due to their universality, distinctiveness, and permanence.[1810] Their reliable nature has been confirmed by the ECJ in the Schwarz case[1811] and more recently in the Landeshauptstadt Wiesbaden case.[1812] The former case concerned an applicant who applied to the city of Bochum for a passport but refused to have his fingerprints taken. In its reasoning, the ECJ held that "the fact that the method is not wholly reliable is not decisive."[1813]

But what does "not wholly reliable" actually mean? The Court's statement concerned fingerprint data, which must be distinguished from facial images, as the former is more accurate. The quality of all types of biometric data can differ greatly.[1814]

The quality of facial images depends on the conditions under which they are captured. Different lighting, background composition, or odd angles make it more difficult to compare two images. Such circumstances may

1809 In most cases, unless there is a humanly-made deficiency such as the ones described above, it is not possible for the data subject to unearth how an error was made and whether it's a technical or human one.

1810 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 398; Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (n 35).

1811 *Michael Schwarz v Stadt Bochum* (n 547).

1812 Case C-61/22 *RL v Landeshauptstadt Wiesbaden* [2024] C/2024/3129.

1813 *Michael Schwarz v Stadt Bochum* (n 547), para 43.

1814 A biometric is a physical or biological feature or attribute that can be measured through a statistical process: EU Commission Joint Research Centre, 'Biometrics at the Frontiers: Assessing the Impact on Society - for the EU Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)' (Institute for Prospective Technological Studies 2005) EUR 21585 EN.

cause a mistake in identification.[1815] Other factors can be extreme temperature and humidity, inhomogeneous illumination, or scalability problems.[1816] Moreover, facial recognition software performs worse on some persons than on others. Darker-skinned female faces between 18 and 30, e.g., are the most difficult to identify.[1817] Research investigating current state-of-the-art facial recognition systems also found a negative bias and considerable degradation in performance for algorithms deployed on children, compared to the performance obtained in adults.[1818] Contrary to general expectations, a large data set might decrease the accuracy of facial recognition due to the higher probability of lookalike subjects in the enrolled image set. However, the same research also shows that the progress in the design of face algorithms implied a continuous improvement of recognition rates over time, meaning that facial recognition is getting more accurate.[1819]

Similarly, different angles or pressures when taking fingerprints and humidity or a dry environment can influence the quality of fingerprint data.[1820] The same goes if fingerprints are less pronounced due to manual and rural labour.[1821] Fingerprint samples can also be more difficult to collect for persons of darker skin colour or for persons with disabilities.[1822] Finally, the age of the data subject is an important factor relating to the accuracy of fingerprint comparison. A study by the European Commission on automatic fingerprint recognition shows that fingerprints of adults become less reliable from the age of 43 years. Fingerprints of children up to the age

1815 Feldmann, 'Considerations on the Emerging Implementation of Biometric Technology' (n 1353) 663.

1816 Sanchez del Rio José, Moctezuma Daniela, Conde Cristina et al. 'Automated border control e-gates and facial recognition systems' (2016) 62 Computers & Security 56.

1817 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research* (2018); Alex Najibi, 'Racial Discrimination in Face Recognition Technology' (*Science in the News*, 24 October 2020) <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/> Kaurin, 'Data Protection and Digital Agency for Refugees' (n 1353) 8.

1818 Nisha Srinivas and others, 'Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults' (2019).

1819 Herrero Galbally, Pasquale Ferrara, Rudolf Haraksim, et al., 'Study on Face Identification Technology for Its Implementation in the Schengen Information System' (*European Commission,* 23 July 2019) 65.

1820 Feldmann, 'Considerations on the Emerging Implementation of Biometric Technology' (n 1353) 663.

1821 Kaurin, 'Data Protection and Digital Agency for Refugees' (n 1353) 8.

1822 ibid 8.

of 12 years are not very reliable. Fingerprint quality of children increases between zero and twelve years of age. From twelve years old until 17, fingerprint quality becomes stable and is considered equal to that of adults between 18 and 25.[1823] Nevertheless, the Explanatory Memorandum for the Eurodac Regulation Proposal of 2016 based its use of young children's biometric data on a study conducted in 2013 by the Commission's Joint Research Centre. This study indicates that fingerprints taken from children aged six and above can be used in automated matching scenarios such as Eurodac, when sufficient care is taken to acquire good quality images.[1824] In an FRA report, experts also expressed concern about the reliability of a fingerprint match when a long period of time has passed since a child's fingerprint was first taken.[1825] In terms of fingerprint quality, the most challenging age group are the elderly, 65 years of age and above. This demographic presents an overall quality significantly lower than that of children. The fingerprint quality for a 65-year-old person is similar to that of a four-year-old child.[1826]

There is a whole range of other factors that can influence the quality of data and their comparability. The challenges of poor data quality are magnified by resource constraints, political instability, or inadequate infrastructure.[1827] A study conducted in the hotspots has also shown that the monitoring and supervision of data processing and sharing procedures can be inadequate and fragmented.[1828]

Given the above, it is difficult to understand how the reliability of biometric data can be considered "not decisive". It should also be acknowledged that even fingerprint and facial recognition systems with very low misidentification rates can impact a large number of individuals when

1823 Herrero Galbally, Pasquale Ferrara, Rudolf Haraksim, et al., 'Study on Face Identification Technology for Its Implementation in the Schengen Information System' (*European Commission,* 23 July 2019) 65.

1824 2016 Eurodac Proposal 'Explanatory Memorandum' 13 referring to Schumacher Guenter, 'Fingerprint Recognition for Children' (Institute for the Protection and Security of the Citizen 2013) JRC85145.

1825 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 116.

1826 Beslay Laurent, Javier Galbally and Rudolf Haraksim, 'Automatic Fingerprint Recognition: From Children to Elderly - Ageing and Age Effects' (European Commission 2018) JRC110173, 34ff.

1827 Leese 'Between control and empowerment: Data quality in border and migration management' (n 64) 6.

1828 Sarah Tas 'Datafication of the hotspots in the blind spot of supervisory authorities' (2024) 30 European Law Journal 87ff.

applied to extensive datasets. For example, a false positive identification rate of 0.01 means that among 100,000 people, 1,000 will be erroneously identified.[1829] From a technical point of view, this may be a success. In legal terms, however, this means that in a country like Germany, where more than 250,000 people applied for asylum in 2022,[1830] 2,500 people could be misidentified and potentially initiate proceedings, which is a huge number to absorb.

What is more, AI algorithms can process vast amounts of data because they previously compressed such information. Data compression mechanisms may imply the loss of differences and peculiarities within the reality under analysis.[1831] As mentioned, Eurodac might contain low-quality data with spelling errors, erroneous birth dates or biometric data recorded in far from ideal circumstances and with a lack of training in dealing with digital infrastructures. AI algorithms receiving data inputs with such flaws will logically deliver unreliable outcomes.[1832]

The untested belief in the infallibility of biometric identifiers can be challenged by numerical evidence. In a 2021 study, it has been reported that

1829 A distinction has to be made between so-called 'false positive' identification and 'false negative'. A 'false positive' refers to the situation where an image is falsely matched to another image. In a migration law context, this would mean that e.g. an asylum seeker is wrongly identified as a someone who already entered the Schengen Area illegally some years earlier, or that a person is wrongly identified as being on the ETIAS watchlist. This has crucial consequences on that persons' fundamental rights. The "false positive identification rate" gives the proportion of erroneously found matches (e.g. number of people on the watchlist identified who are in fact not on the watchlist) among all those who are not on the watchlist. 'False negatives' are those who are deemed not to be matches (i.e. not on the watchlist), but in fact are matches. The corresponding "false negative identification rate", or "miss rate", indicates the proportion of those erroneously not identified among those who should be identified. Cf FRA, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (2019) 9; cf also NIST, 'Face Technology Evaluations - FRTE/FATE' (5 May 2024) <https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate> accessed 5 May 2024; Dana Michalski and others, 'The Impact of Ageing on Facial Comparisons with Images of Children Conducted by Humans and Automated Systems' (2017) 21ff, according to which only 87 false hits were reported by Member States in 2021. This is, however, only the number of false hits reported, not the actual number of false hits.

1830 Bundesamt für Migration und Flüchtlinge, 'Das Bundesamt in Zahlen 2022 - Asyl, Migration Und Integration' (2023) 7.

1831 Forti 'Addressing Algorithmic Errors in Data-Driven Border Control Procedures' (n 30) 638.

1832 ibid 639.

16% of inquiries in Eurodac resulted in a hit. In 10% of those cases, the biographic data were found to be inadequate, and in 4.5% of cases the quality of the fingerprints acquired was too weak.[1833] According to the Eurodac Annual Report by eu-LISA, in the year 2022 overall, 36,946 data sets under Category 1 and 2 were rejected by Eurodac due to insufficient quality, which is 3.11%; a slight decrease from 3.98% in 2021.[1834] Additionally, 4.25% of transactions, this means 112,407 entries, updates or deletions, were rejected due to errors. This is quite a significant decrease from 9.34% in 2021.[1835] Since 2017, each year only between 84 and 111 false hits were reported.[1836] The number has been increasing over the years.[1837]

It should be noted that these figures reflect errors and rejected transactions under the previous Eurodac Regulation, which included only very limited information and solely fingerprint biometrics. This is set to change, and it can be expected that the incidence of inaccurate data will increase. According to an Italian NGO, in half of the asylum cases originating from southern hotspots, the recorded personal identity data are incorrect.[1838] In practice, even small discrepancies with identity data can, in some cases, be used as a reason to reject an asylum request altogether.[1839]

The CJEU has underlined that even if trust regarding the protection of fundamental rights and EU law can be assumed, there is no such principle of "blind trust".[1840] Nevertheless, the assumption that the partial unreliability of biometric data is "not decisive" appears to reflect a form of

1833 Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 399.

1834 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 25.

1835 ibid 25.

1836 eu-LISA, 'Eurodac 2021 Annual Report' (n 990) 23.

1837 ibid 23.

1838 Mark Latonero and others, 'Digital Identity in the Migration & Refugee Context: Italy Case Study' (Data and Society Research Institute 2019) 25.

1839 Some Member States have takes measures against a practise of direct return of persons, whose identitiy could not be corroborated. In Germany, e.g., exists a temporary residence status for persons whose identity could not be clarified (Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet 1) [2005] (Aufenthaltsgesetz - AufenthG), § 60b Duldung für Personen mit ungeklärter Identität).

1840 cf Eveline Brouwer and Damian Gerard (eds), 'Mapping Mutual Trust: Understanding and Framing the Role of Mutual Trust in EU Law' (European University Institute 2016) Working Paper MWP 2016/13; Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (n 55).

blind trust. What is crucial, particularly in the context of algorithmic or automated decision-making, is how human decision-makers interpret and rely on such technical inputs. The way human decision-makers perceive algorithmic information – whether they treat it as authoritative or not – and their level of expertise, for example as skilled professionals or untrained administrators, shape the interaction between humans and machines and affect the balance of autonomy and responsibility in decision-making.[1841] A key element in this dynamic is the symbolic power of algorithms as an 'objective', neutral application of data to rules.[1842] In the context of Eurodac, it must be assumed that the results of data comparisons are perceived as authoritative, and that the system is primarily used by individuals with limited understanding of the underlying technology. This study therefore makes two arguments. First, it must be possible to effectively challenge the accuracy of data comparisons. Second, where data are systematically incorrect due to human practices – for example, when minors are routinely registered as adults – mutual trust must be set aside.

c) *Intensity of Review*

The previous section has demonstrated that trust in both Eurodac data and the associated processing operations is very high. Eurodac hits – that is, data matches – are treated as conclusive proof.[1843] This raises critical questions: what type of evidence can be submitted in proceedings challenging the accuracy of Eurodac data? And how thorough must a legal review be when assessing such evidence?

The case law of the CJEU has not examined in detail what constitutes a 'full review' under Art. 47 CFR.[1844] The ECJ held, in the case Wilson,

1841 Paul W Fay Henman, 'Administrative Justice in a Digital World: Challenges and Solutions' in Joe Tomlinson and others (eds), *The Oxford Handbook of Administrative Justice* (Oxford University Press 2021) 436.

1842 ibid 436; cf also Tarleton Gillespie, 'The Relevance of Algorithms' in Pablo J Boczkwoski and Kirsten A Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (The MIT Press 2014); Rob Kitchin, 'Thinking Critically about and Researching Algorithms' (2016) 20 Information, Communication & Society 14.

1843 cf Dublin III Implementing Regulation, Annex II; see also next section: d) Burden and Standard of Proof.

1844 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.185; but ibid, no 47.187, states that "[t]he standards of the duty of care so

that review by an independent tribunal that was limited to questions of law and did not extend to a review of the facts, was insufficient.[1845] The preclusion of reviewing certain types of evidence submitted to the referring court would likewise constitute a breach of Art. 47 CFR.[1846] Authorities must examine, carefully and impartially, all the relevant elements of the situation in question.[1847] According to the CJEU, in complaint procedures, the procedural right to a careful investigation has to be distinguished with caution from substantive questions of law. It shall not be used as a container principle which minimises substantive, administrative discretion.[1848] With the help of the concept of the 'duty of care', which has been discussed above, the CJEU reviews whether all relevant information from a qualitative and a quantitative point of view has been taken into account and whether, cognitively, a decision could have been based on such facts.[1849] Union courts have to establish, amongst other things, whether the evidence relied on is factually accurate, reliable and consistent. They must further establish whether it contains all the information that must be considered in order to assess a complex situation and whether it is capable of substan-

---

far established are thus also the standards interpreted to be required under the principle of effective judicial protection as general principles of EU law. Under these standards, expertise such as technical and scientific specialist knowledge cannot, according to the CJEU, be subject to judicial review per se but must be framed in procedural terms".

1845 *Graham J Wilson v Ordre des avocats du barreau de Luxembourg* (n 1532), para 62.

1846 Case C-437/13 *Unitrading Ltd v Staatssecretaris van Financiën* [2014] OJ C 439/10, para 25.

1847 Case C-62/14 *Peter Gauweiler and Others v Deutscher Bundestag* [2015] OJ C 279/12, para. 69; cf also Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.184 ff; Case C-544/15 *Sahar Fahimian v Bundesrepublik Deutschland* [2017] OJ C 168/12; referring to Joined Cases C-379/08 and C-380/08 *ERG and Others* [2010] OJ C 113/10; and *Peter Gauweiler and Others v Deutscher Bundestag* (n 1847), para 69. See also on Art 47 CFR, and the need to review facts, law, and procedures: Case C-89/17 *Secretary of State for the Home Department v Rozanne Banger* [2018] OJ C 319/9, para 51. On Art. 47 and the duty of Member State courts to verify relevant facts in the light of criteria set in a directive see e.g., Case C-723/17 *Lies Craeynest and Others v Brussels Hoofdstedelijk Gewest, Brussels Instituut voor Milieubeheer* [2019] OJ C 280/4.

1848 Herwig CH Hofmann, Rowe C Gerard and Alexander Türk, *Administrative Law and Policy of the EU* (3rd edn, Oxford University Press 2012) 447ff with references.

1849 Hofmann, 'Article 47 - Right to an Effective Remedy and to a Fair Trial' (n 559), no 47.183; cf also Jens-Peter Schneider, 'Basic Structures of Information Management in the European Administrative Union' (2014) 20 European Public Law 89.

tiating the conclusions drawn from it.[1850] In addition, in the fact-finding process the authorities should observe procedural safeguards, in particular the right to be heard of the persons concerned.[1851] However, as pointed out by Widdershoven, the CJEU's case law shows that Art. 47 CFR does not require one uniform standard of judicial review in all cases but that the precise intensity depends on the applicable Union rules.[1852]

The intensity of judicial review of proportionality in cases involving interferences with fundamental rights – and in particular the right to respect for private life under Art. 7 CFR and the related protection of personal data under Art. 8 CFR – was examined by the ECJ in Digital Rights Ireland.[1853] The ECJ states that wherever interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference, and the object pursued by the interference.[1854] From the subsequent case of Tele2 Sverige, it can be derived that the judicial review by the national court of a national act seriously interfering with the fundamental rights of Art. 7 and Art. 8 CFR should be as strict as the judicial review of such interferences by the ECJ.[1855] The principle of procedural autonomy for national courts does not apply.[1856]

Recent cases in the field of immigration and asylum law set standards which, as pointed out by Advocate General Bobek in the Torubarov case, "constitute an expression of more general principles related to the require-

1850 Case C-12/03 *Commission of the European Communities v Tetra Laval BV* [2005] ECR I-987, para 39.

1851 Rob Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' in Jurgen de Poorter, Ernst Hirsch Ballin and Saskia Lavrijssen (eds), *Judicial Review of Administrative Discretion in the Administrative State* (TMC Asser Press 2019) 56; with reference to *Commission of the European Communities v Tetra Laval BV* (n 1796); and *Technische Universität München v Hauptzollamt München-Mitte* (n 1298).

1852 Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' (n 1851) 49.

1853 *Digital Rights Ireland Ltd v Minister for Communications and Others* (n 730), paras 46 - 48.

1854 ibid, para 47; As regards this standard of judicial review the ECJ refers, by analogy, to: *S and Marper v United Kingdom* (n 732), para 102.

1855 *Tele2 Sverige* (n 522); Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' (n 1851) 47.

1856 Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' (n 1851) 47.

ment of effective judicial remedy" in Art. 47 CFR and Art. 19(1) second sentence TEU.[1857] In the case of Samba Diouf, the ECJ obliged the national courts to exercise, in asylum cases, a "thorough review" of the legality of the decision and, in particular, of the reasons that led the competent authority to reject the application for asylum as unfounded.[1858] The notion of full judicial review in view of Art. 47 CFR, according to the CJEU, means, in asylum cases, that the court or tribunal is required to examine both the evidence that the determining authority took into account or could have considered if it had properly made a decision.[1859] It should be noted that this view is not shared by all Member States.[1860] The ECtHR also

1857 Case C-556/17 *Alekszij Torubarov v Bevándorlási és Menekültügyi Hivatal* [2019], Opinion of AG Bobek, para 48; Torubarov however addressed the exceptional case, where the CJEU held that it might be necessary that a Court be 'required to vary a decision of the administrative or quasi-judicial body' and to 'substitute its own decision' in order to ensure compliance with the principle of effective judicial protection in only the most exceptional cases where an administration does not comply with a previous judgment: Case C-556/17 *Alekszij Torubarov v Bevándorlási és Menekültügyi Hivatal* [2019] OJ C 319/8, para 74.

1858 *Brahim Samba Diouf v Ministre du Travail, de l'Emploi et de l'Immigration* (n 1613), para 56.

1859 Hofmann, 'The Duty of Care in EU Public Law – A Principle Between Discretion and Proportionality' (n 1682) 22 referring to Case C-585/16 *Serin Alheto v Zamestnik-predsedatel na Darzhavna agentsia za bezhantsite* [2018] OJ C 328/6, paras 113 and 114.

1860 In the Netherland, for example, there has been a lively debate as regards the question how strict ('full') the 'full examination of facts and law' should be. Some scholars argue that a full examination should be 'unlimited'. Therefore national courts should not conduct a legality review of the decisions taken by the asylum authorities only, but should substitute their own appraisal of the facts that might constitute a right to asylum for that of the authorities (for instance: Raad van State, 13 april 2016, Reneman, 201507952/1/V2 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 14 oktober 2015 in zaak nr. 15/17328*); and Raad van State, 13 april 2016, 201601482/1/V2 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Roermond, van 22 februari 2016 in zaak nr. 16/1367)*); The Dutch Council of State has rejected this view and has determined that the authorities still enjoy some discretion as regards the appraisal of uncertain facts, more in particular in respect of whether the statements of person seeking asylum are plausible (201507952/1/V2 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Zwolle, van 14 oktober 2015 in zaak nr. 15/17328* (n 1860)) and 201601482/1/V2 *(appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Roermond, van 22 februari 2016 in zaak nr. 16/1367)* (n 1860)); According to the Council of State this discretion—and the judicial deference resulting from it – is justified by the fact that the authorities have more expertise in assessing the plausibility of such statements, because they have an overview of all asylum decisions, including decisions granting asylum.

applies, in the context of asylum and return procedures, a relatively high 'intensity' of review under Art. 13 ECHR.[1861] It does not explicitly require that, in addition to the evidence taken into account, evidence that could have been taken into account must be considered. With regard to Art. 3 ECHR cases, an investigation must, however, be "effective" in practice as well as in law, and not be unjustifiably hindered by the acts or omissions of the authorities of the respondent state.[1862] In M.S.S v Belgium and Greece, the Court stated that in cases regarding Art. 3 ECHR, while leaving a certain margin of appreciation to the states, conformity with Art. 13 ECHR requires that the competent body "must be able to examine the substance of the complaint".[1863] With regard to transfer decisions, the CJEU leaves the intensity of the review mostly in the hands of the Member States.[1864]

A rather restrained judicial review was applied in the already discussed ECJ case of Berlioz, due to the principle of mutual trust.[1865] The Luxembourg authorities were only permitted to verify whether the information requested by the French authorities "is devoid of any foreseeable relevance" to the French investigation.[1866] The Court did not leave any room for the national courts to apply a (possibly) stricter judicial standard on the basis of its national law.[1867]

In summary, depending on the circumstances of a Eurodac case, the intensity of judicial review may vary. Generally, the evidence relied upon should be factually accurate, reliable, and consistent, encompassing all

---

As means of compensation the Council of State prescribes to the first instance courts a strict procedural test of the fact-finding process and of the statement of reasons: Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' (n 1851) 51.

1861 The notion of an effective remedy requires independent scrutiny of the claim that there exist substantial grounds for fearing a real risk of treatment contrary to Article 3, given the irreversible nature of the harm that might occur if the risk of ill-treatment materialised. This scrutiny must be carried out without regard to what the person may have done to warrant expulsion or to any perceived threat to the national security of the expelling State *(Chahal and Others v United Kingdom* (n 1308), para 151).

1862 *Batı and Others v Turkey* [2004] ECHR 2004-IV, para 134.

1863 *M.S.S v Belgium and Greece* (n 1468), para 387.

1864 *H.A v État belge* (n 1806), para 39ff.

1865 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* (n 1530), para 83ff.

1866 ibid, paras 78, 82 and 86.

1867 ibid; Widdershoven, 'The European Court of Justice and the Standard of Judicial Review' (n 1851) 51.

information necessary to assess a complex situation and substantiate the conclusions drawn. When asylum is at issue, the data subject must be allowed to present all possible evidence, and courts may even need to consider evidence that could have been presented but was not. However, how this standard applies to data and technical processes, such as errors in AI, remains unclear. This is particularly challenging given that "AI programs continuously adapt their cognitive processes in response to changing external conditions, making it technically challenging to identify errors and trace their underlying causes".[1868]

d) *Burden and Standard of Proof*

As discussed in the previous chapters, an access to information request generally does not require the data subject to provide reasons or evidence. However, when requesting the rectification or erasure of data – such as an incorrect Eurodac record, a Eurodac hit arising from such a record, or a contested security flag – evidence becomes necessary. In these cases, questions arise regarding who bears the burden of proof, what must be proven, and how such proof can be presented.

aa) With Regard to Biometric or Biographic Data and Eurodac Hits

Art. 22 of the Dublin III Regulation, as further detailed in the Commission's Dublin III Implementing Regulation, distinguishes between probative (formal) evidence and circumstantial evidence regarding a Member State's responsibility to process an application for international protection. This distinction has been adopted by the AMMR.[1869] Eurodac hits are classified within the category of probative evidence.[1870] Other examples of probative evidence include a written report from the authorities of another Member State confirming that an application has been submitted, as well

1868 Forti 'Addressing Algorithmic Errors in Data-Driven Border Control Procedures' (n 30) 644.
1869 AMMR, Art 19(1)(s), 33, 40 and Recital 54.
1870 Dublin III Implementing Regulation, Art 2 and Annex II.

as extracts from registers and official files.[1871] Circumstantial evidence can include verifiable statements by the applicant, such as in the Dublin interview, reports from UNHCR or other international organisations, and statements by family members.[1872] Member States should weigh both probative and circumstantial evidence when determining responsibility.[1873] In a study by the European Commission, Member States confirmed that they tend to give preference to probative evidence, even stating that Eurodac evidence is given top priority.[1874] Some Member States rely only on Eurodac hits when considering a request or only accept Eurodac hits, especially Member States that receive take backs.[1875] Sometimes, a lack of trust between Member States pre-exists. A hit may not result in a transfer, as certain Member States assume responsibility in accordance with Art. 17 Dublin III Regulation (replaced by Art. 25 AMMR).[1876] Reliance on technologies has furthermore led, in some cases, to the prioritisation of a Eurodac hit over the investigation of family ties, thus jeopardising the hierarchy of the Dublin criteria.[1877] Member States should consider both probative and circumstantial evidence.[1878] Judicial review in asylum cases may require that even evidence that could have been taken into account (but wasn't) has to be considered.[1879]

Neither the Eurodac and Interoperability Regulations nor the GDPR explicitly allocate the burden of proof regarding the accuracy of Eurodac data. Consequently, it must be determined according to general principles, taking into account the fundamental rights referenced in Art. 1(2) GDPR and the principle of data accuracy under Art. 5(1)(d) GDPR, including the controller's accountability under Art. 5(2) GDPR. The data subject must demonstrate that the data are inaccurate, while the Member State bears the

1871 ibid, Annex II; This will be replaced by a new Commissions Act, according to AMMR, Art 40(4). It is to be expected that what counts as proof and circumstantial evidence will be similar and stay the same with regards to Eurodac hits.
1872 ibid.
1873 DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (n 695) 25.
1874 ibid 25ff.
1875 ibid.
1876 ibid 36.
1877 ibid 31.
1878 ibid 25.
1879 *Serin Alheto v Zamestnik-predsedatel na Darzhavna agentsia za bezhantsite* (n 1859), paras 113 and 114; Hofmann, 'The Duty of Care in EU Public Law – A Principle Between Discretion and Proportionality' (n 1682).

burden of proving the accuracy of the data, as it is obliged to process only factually correct information under Art. 5(1)(d) GDPR.[1880] Data subjects are only required to dispute the accuracy of the data. The threshold for contesting data accuracy should not be set too high. Nonetheless, at a minimum, data subjects must indicate which specific data they allege to be incorrect.[1881]

According to some scholars, Member States are required to rectify or erase data without delay, if they cannot prove their accuracy and the data subject cannot prove their inaccuracy.[1882] Others suggest the permanent restriction of processing for such data.[1883] Since the new Eurodac Regulation contains an explicit right to restriction of processing of data, Member States might not be required to erase data in case of a *non liquet* but can permanently restrict its use.[1884]

Under Eurodac Regulation 603/2013, a Eurodac hit was defined as a match resulting from fingerprint data comparison.[1885] With the new Eurodac Regulation, a wider range of data – particularly biographical informa-

1880 Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), para 15; Hans-Georg Kamann and Martin Braun, 'Art. 16 - 21' in Eugen Ehmann and Martin Selmayr (eds), *DS-VCG: Datenschutz-Grundverordnung, Kommentar* (3rd edn, CH Beck 2024), para 21; similar Boris Paal and Daniel Pauly (eds), *Datenschutz-Grundverordnung | Bundesdatenschutzgesetz* (2nd edn, CH Beck 2018), para 15. With regard to the right to restricting of processing, cf Tobias Herbst, 'Artikel 18 - Recht auf Einschränkung der Verarbeitung' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd edn, CH Beck 2020), para 13; and Domingos Farinho, 'Article 18 - Right to Restriction of Processing' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou and Gerrit Hornung (eds), *General Data Protection Regulation - Article by Article Commentary* (1st edn, Nomos 2019), para 8, where it is also stated that the data subject must contest the accuracy of the data, which mandates the controller to verify the claim according to the principle of accuracy (Art. 5(1)(d)) and Art. 16. In para 9, however, Farinho states that the burden of proof falls on the controller due to Art. 5(2) GDPR.

1881 Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), para 16 with references.

1882 Dix, 'Artikel 18 - Recht auf Einschränkung der Verarbeitung' (n 1238), no 5; Herbst, 'Artikel 18 - Recht auf Einschränkung der Verarbeitung' (n 1880), para 13; Farinho, 'Article 18 - Right to Restriction of Processing' (n 1880), no 8.

1883 Peuker, 'Artikel 16 - Recht auf Berichtigung' (n 1238), Art 16, no 17 and Art 18, no 12; similarly, Farinho, 'Article 18 - Right to Restriction of Processing' (n 1880), no 9 suggests that the case ought to be brought before the DPA (GDPR, Art 77), which may order a new assessment of the accuracy or restict processing (Art. 58(2)(d) and (g), respectively).

1884 Eurodac Regulation 2024, Art 43.

1885 Eurodac Regulation 603/2013, Art 2(1)(d).

tion and facial images – will be collected and stored. In most cases, a hit will still indicate a match of biometric data, whether fingerprints or facial images recorded in Eurodac and transmitted by a Member State.[1886] Additionally, according to Art. 32 of the Eurodac Regulation, for law enforcement purposes, comparisons will include not only biometric but also alphanumeric data.

A distinction must be drawn between the two categories of Eurodac data: biometric and biographic. In the case of a Eurodac hit based on biometric data, the hit constitutes probative evidence, as the Eurodac and Interoperability Regulations rely heavily on trust in the technical systems behind such hits. Challenging this evidence requires the data subject to prove the inaccuracy of the hit or the underlying biometric data, which can be particularly difficult. Eurodac hits are generated by an algorithm, and the inherent opacity of (AI) algorithms makes identifying potential errors challenging, thereby limiting the ability of affected individuals to contest administrative decisions.[1887] Moreover, the new Eurodac Regulation has removed a key security feature in the data comparison process: fingerprint experts now review the results of comparisons only "where necessary,"[1888] rather than in every case.[1889] Accordingly, if a data subject disputes a Eurodac hit, the first step should be to assign a fingerprint expert to verify the result. The threshold for triggering such an expert review should not exceed a credible challenge to the Eurodac hit by the data subject.

In the case of biographic data in Eurodac, it is debatable whether such data can constitute full proof if they are not supported by probative evidence, such as a birth certificate or passport. This situation arises, for instance, when asylum seekers travel without documentation. In such cases, the data – and any resulting hit – are based solely on the data subject's oral

1886 Eurodac Regulation 2024, Art 2(1)(j).

1887 Forti 'Addressing Algorithmic Errors in Data-Driven Border Control Procedures' (n 30) 641; The question of whether, and how, AI can and must be explained in a legal context is a subject of considerable debate within legal scholarship, cf Sandra Wachter, Brent Mittelstadt, Luciano Floridi 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law, 76–99); Malgieri Gianclaudio 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' (2019) 35(5) Computer Law & Security Review, 1–26, 2 "Figuring out the reasons behind a specific algorithmic output would make human actors morally accountable for its implementation".

1888 ibid, Art 38(4).

1889 ibid, Art 25(4).

statements, for example during an interview, which amounts to circumstantial evidence. Therefore, if a hit is generated from unverified biographic data, the hit itself cannot be treated as probative evidence, but only as circumstantial. Consequently, the threshold for disputing such a hit should be lower. According to a data controller interviewed in a study by FRA in Germany, rectification of data is usually not complicated if evidence, such as a reliable birth certificate or passport, is presented.[1890] However, there are numerous cases in which data subjects cannot provide probative evidence due to persecution or conflict in their country of origin.[1891] In such situations, a credibility assessment is conducted, often requiring the authorities to weigh different statements made by the data subject. This can work to the disadvantage of the individual. For instance, the Council of State (*Raad van State*) in the Netherlands held that if a foreign national is registered in multiple Member States with differing ages – one or more of which indicates adulthood – it can be concluded that the individual is an adult, and no age assessment test is required.[1892]

The question of standard of proof has been dealt with in two older cases in the UK that provide some interesting insight into how a Eurodac hit can be understood from an evidentiary perspective. In YI in 2007, the Asylum and Immigration Tribunal decided that where "Eurodac data is produced by the respondent in cases such as this essentially to assert deception/fraud by an Appellant. The burden of proof rests with the person making the assertion and the standard of proof where fraud is asserted and where the consequences for the appellant are correspondingly serious is the higher standard of 'proof to a high degree of probability'."[1893] In other words, where fingerprint evidence was used by the respondent to challenge the truth of the account given by the appellant, this was equivalent to an assertion that the asylum claim was fraudulent; for this reason, a high standard of proof was required.

This position was overturned in a later case, RZ, where the Asylum and Immigration Tribunal stated that "when the respondent seeks to rely on fingerprint evidence in an asylum appeal, he is seeking to prove a number of facts: that fingerprints taken in a member state at a specific place, date

1890 FRA, 'Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights' (n 70) 101.

1891 ibid 101.

1892 202104145/1/V1 (*appellant / de uitspraak van de rechtbank Den Haag, zittingsplaats Middelburg, van 23 juni 2021 in zaak nr NL216802*) (n 1446).

1893 YI, *Eritrea v Secretary of State for the Home Department* (n 1198), para 12.

and time are a match with the fingerprints of an appellant taken in the course of his current application. These are issues of fact for the respondent to prove on a balance of probabilities. [...] The assertion that a particular appellant has previously given fingerprints in a member state is not in itself an allegation of forgery or fraud bringing into play the higher civil standard of proof [...] It is an allegation that there is a match between fingerprints held in the Eurodac system. If the match is proved the respondent may well seek to argue that the appellant has not told the truth about material parts of his asylum claim and that his evidence is unreliable in whole or in part [...]". In summary, the burden of proving a fingerprint match from the Eurodac system lies on the respondent and the standard of proof is the balance of probabilities.[1894]

In practice, the latter view has prevailed. In the years since these cases were decided, the technology, especially for the comparison of fingerprints, has improved even further. Today, it is clear that a hit is considered 'proof to a high degree of probability' anyway.[1895]

Blind faith in Eurodac and the interoperability technology can lead to data subjects' complaints about data quality not being heard. This is particularly the case whenever data subjects cannot provide any conclusive evidence. As Feldman put it: "The real problem is not that biometrics are subject to fraud or error, but our conviction nonetheless in its accuracy. Human beings have an almost blind faith in all things scientific, and biometric data is cloaked in the mantle of scientific truth."[1896] A police officer interviewed in Germany for FRA's biometrics project stated that there is a tendency among the staff of the competent authorities to assume that inaccuracies and mismatches are the result of right holders providing false

1894 RZ, *Eritrea v Secretary of State for the Home Department* (n 1474), para 48; similarly, also the England and Wales High Court, who stated that a Eurodac match normally discharges the burden of proof on the Secretary of State and does not need to be corroborated. This puts the onus on the asylum seeker to produce evidence to disprove the match (England and Wales High Court (Administrative Court) - *R (on the application of YZ, MY and YM) v Secretary of State for the Home Department* [2011] EWHC 205.

1895 cf *Michael Schwarz v Stadt Bochum* (n 547), para 43.

1896 Feldmann, 'Considerations on the Emerging Implementation of Biometric Technology' (n 1353) 665. 'Automation bias' has been described for a long time by scholars (cf e.g. Mosier Kathleen, Skitka Linda, 'Automation use and automation bias' (1999) 43(3) Proceedings of the Human Factors and Ergonomics Society Meeting, 344ff.).

information at some point.[1897] It is therefore important that the results of data processing operations can be disputed without excessive hurdles, and that the Member States actually carry their burden of proof. The ECJ ruled that a Member State seeking to have an applicant taken back by the responsible Member State, and wishing to transfer the applicant, must take certain steps before carrying out the transfer. The transferring Member State must consider all information provided by the applicant, especially regarding any real risk of inhuman or degrading treatment during or after the transfer. Furthermore, the two Member States must cooperate to establish and verify the facts surrounding the applicant's claims.[1898] The applicant must have the opportunity to present all information that is relevant to correctly determine the Member State responsible and to provide any relevant elements of proof or any circumstantial evidence.[1899] According to the Court, the Dublin III Regulation makes clear that the requirement of proof should not exceed what is necessary for the proper application of that regulation and that, if there is no formal proof, the requested Member State is to acknowledge its responsibility, if the circumstantial evidence is coherent, verifiable, and sufficiently detailed to establish responsibility.[1900]

bb) With Regard to Security Flags

The burden of proof for establishing that a data subject poses a threat to internal security rests with the Member State of origin. If that Member State determines that the threat no longer exists, it must delete the security flag from the data set. This must be done after consulting any other Member States that have registered a data set for the same individual.[1901] As has been established earlier in this study, parts of a security flag may be considered police information, others intelligence information.[1902] Access to data can be restricted in accordance with Art. 23 GDPR.

1897 FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674) 33; similar also the idea of migrants a trickster and deceivers, as describe by Scheel Stephan, 'Reconfiguring Desecuritization: Contesting Expert Knowledge in the Securitization of Migration' (2022) 27(4) Geopolitics, 1042ff.

1898 *X v Staatssecretaris van Justitie en Veiligheid* (n 1426).

1899 ibid, para 71ff.

1900 ibid, para 74.

1901 Eurodac Regulation 2024, Art 17(4).

1902 See chapter: The Right to Information.

With regard to the right to an effective remedy, it is important to underline that the data subject has to be able to access or receive enough information on the security flag to be capable of defending themselves against it. In its leading case, ZZ, on access to evidence in national security cases, the ECJ makes clear that the right to an effective remedy of a person can only be limited to the extent that is strictly necessary; the applicant must be informed – at a minimum – of the essence of the grounds on which the decision is founded.[1903] This case concerned the refusal of an entry permit on the basis of security-related evidence – a constellation that is also conceivable in connection with security flags.[1904] The Court stated that the fundamental right to an effective legal remedy would be infringed if a judicial decision were founded on facts and documents that the parties themselves, or one of them, have not had an opportunity to examine, and on which they have therefore been unable to state their views.[1905] Only if, "in exceptional cases, a national authority opposes precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision […], by invoking reasons of State security, the court with jurisdiction in the Member State concerned must have at its disposal and apply techniques and rules of procedural law which accommodate, on the one hand, legitimate State security considerations regarding the nature and sources of the information taken into account in the adoption of such a decision and, on the other hand, the need to ensure sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle."[1906]

In another ECJ case, R.N.N.S, visas were refused in two unrelated cases, based on information from Member States other than the ones the two applicants were applying to. The refusal was notified to them by means of a standard form. However, the forms sent to the applicants concerned did not provide any indication of the identity of those Member States, the specific ground for refusal out of the four possibilities, or the reasons they had been considered to be such a threat.[1907] The Court decided that the

1903 *ZZ v Secretary of State for the Home Department* (n 559).
1904 ibid, para 22ff.
1905 ibid, para 56, with reference to *Digital Rights Ireland Ltd v Minister for Communications and Others* (n 730), para 52.
1906 ibid, para 56; referencing, by analogy, Case C-402/05 *P Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* [2008] ECR I-6351, para 344.
1907 *R.N.N.S and KA v Minister van Buitenlandse Zaken* (n 1088), para 12ff.

Member State refusing the visa is required to indicate, in that decision, the identity of the Member State which raised that objection, the specific ground for refusal based on that objection, accompanied, where appropriate, by the essence of the reasons for that objection.[1908] The final decision for refusing a visa will have to indicate the authority which the applicant may contact in order to ascertain the remedies available to that end in the other Member State.[1909] Similarly, in GM v Országos Idegenrendézeti Főigazgatóság, the ECJ had to rule on the withdrawal of international protection due to a danger to national security. The Court recalled that, "[…], where Member States restrict access to information or sources the disclosure of which would jeopardise, in particular, national security or the security of those sources, the Member States must not only make access to such information or sources available to the courts having jurisdiction to rule on the lawfulness of the decision on international protection, but also establish in national law procedures guaranteeing that the rights of defence of the person concerned are respected".[1910] The person subject to a decision on international protection must be able to acquaint themselves with the elements of their file, which are made available to the court or tribunal called upon to rule on the appeal against that decision.[1911] The Court emphasised that the rights of the defence are, however, not absolute. The right of access to the file, which is a key part of those rights, can be restricted. This limitation is based on a balance between several factors. On the one hand, there is the right to proper administration and the right to an effective remedy for the individual concerned. On the other hand, there are the interests used to justify withholding elements of the file from that person, particularly when those interests involve national security.[1912] It concluded that Art. 47 CFR would "preclude national legislation which provides that, where a decision rejecting an application for international protection or withdrawing such protection is based on information the disclosure of which would jeopardise the national security of the Member State in question, the person concerned or his or her legal adviser can access that information only after obtaining authorisation to that end, are not

1908 ibid, para 57.
1909 ibid, para 52.
1910 *GM v Országos Idegenrendézeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ* (n 1082).
1911 ibid, para 49.
1912 ibid, para 50; referring to that effect to *ZZ v Secretary of State for the Home Department* (n 559), paras 54, 57 and 64, and the case law cited.

provided even with the substance of the grounds on which such decisions are based and cannot, in any event, use, for the purposes of administrative procedures or judicial proceedings, the information to which they may have had access".[1913]

The ECtHR in Muhammad and Muhammad v Romania, in a similar fashion, clarified the procedural safeguards relating to the expulsion of aliens based on national security. Two general principles were highlighted by the Court: first, the safeguards provided is are important when the information given to the person is limited; second, whenever there are particularly significant repercussions for the person's situation, the counterbalancing safeguards must be strengthened accordingly.[1914,1915]

These considerations also apply in cases involving a security flag. Data

1913 *GM v Országos Idegenrendézeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ* (n 1082), para 60.

1914 *Muhammad and Muhammad v Romania* (n 1084), para 146. In summary the Court also held that it must be determined whether the national authorities have, to the extent compatible with maintaining the confidentiality and proper conduct of investigations, informed the alien concerned, in the proceedings, of the substance of the accusations against him or her. A further question of importance is whether it falls upon a judicial or other independent authority to determine, in a given case, after examining all the classified evidence, which factual information may be disclosed to the alien concerned without endangering national security, provided it is disclosed at a stage of the proceedings when the alien is still able meaningfully to challenge that information (para 152). It must be ascertained whether the domestic authorities have provided the requisite information to the alien, at least at key stages in the proceedings. Such information would particularly be useful where aliens are not represented by a lawyer and where a lack of relevant information may result in their failure to exercise rights available to them in domestic law. This will be all the more important in cases where the rules of domestic procedure impose a certain expedition in the examination of the case (para 153). And finally, with regard to representation First, domestic law should afford an effective possibility of representation. The possibility for an alien to be represented by a lawyer, or even by a specialised lawyer who holds the relevant authorisations to access classified documents in the case file which are not accessible to the alien, constitutes a significant counterbalancing factor. Second, the Court will consider whether it was possible in practice for the alien to have effective access to such representation in the course of the proceedings in question. Third, the rights enjoyed by the alien's representative in a given case is a further significant safeguard: for example, the extent to which access to the documents in the case file, including the classified ones, was provided to the representative, and whether or not the representative's communication with the alien was restricted once the access to the classified material had been obtained (para 154 ff).

1915 For an overview of the situation in the Member States cf Katalin Juhász, 'The Right to Know in the European Union: Comparative Study on Access to Classified Data

subjects must have the opportunity to defend themselves and, particularly when the underlying hit originates from a national database, be informed which Member State is responsible. If the hit is not based on a national database, they should at least know which other database produced it. It should be noted that a security flag merely indicates that a person "could" pose a threat. Therefore, the rejection of an application for international protection must be exceptionally well justified, as it may involve a data subject who is potentially being persecuted. Some scholars even demand that the data subject has to be able to trace the source of information that led to the conclusion of them being a security threat.[1916]

This raises the question of the applicable standard of proof: how must it be demonstrated that a person constitutes a security threat, or conversely, that they do not? A security flag is only recorded in Eurodac if the data subject is "violent or unlawfully armed or where there are clear indications that the person is involved in any of the offences referred to in Directive (EU) 2017/541 or in Council Framework Decision 2002/584/JHA".[1917]

The criterion of "unlawfully armed" seems quite clear, as does the evidence to the contrary. If an illegal weapon is found on a data subject, without them having a license for carrying it, the requirement is met. Evidentiary questions arise, however, if the individual asserts that the weapon wasn't theirs, or that they were unknowingly transporting it. This evidence would have to be provided by the data subject and would likely require a high degree of probability.

The Member State bears the burden of proving "clear indications" of involvement in a specified terrorist offence. "Clear" in this context must mean comprehensible and precise indications, which indicates a high standard of proof. At a minimum, the Member State must be able to present circumstantial evidence that credibly points to the individual's involvement.

The criterion of whether a data subject can be considered "violent" is the most difficult to assess. Recital 8 of the Eurodac Regulation clarifies that a Member State must determine whether an individual has engaged in behaviour causing physical harm to others, which would constitute a criminal offence under national law. This excludes acts such as climbing over or damaging a border fence when no individual is harmed. However,

---

in National Security Related Immigration Cases' (Hungarian Helsinki Committee 2024).

1916 Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non- Discriminatory Approach of Data Protection' (n 73) 86.

1917 Eurodac Regulation 2024, Art 17(2)(1), 22(3)(d), 23(3)(e) and 24(3)(f).

under national law, physical violence may be presumed if, for example, a person resists arrest using some degree of physical force. Such incidents, for instance during irregular border crossings, present serious evidentiary challenges: the accusation may originate from a border official, with no documentation, no witness statements, and without the data subject having the opportunity to comment. Importantly, it is not necessary that criminal charges are filed; the assessment only requires that the conduct "would" amount to a criminal offence under national law. Situations may therefore arise in which violent behaviour is alleged without police records, documentation, or procedural safeguards of a criminal procedure such as access to evidence. It is argued that the Member State should provide proof of physical harm, for example via photographs or medical reports, rather than relying solely on an official's statement. In other words, the burden of proof must lie with the Member State to substantiate the claim that the data subject is violent. Without this, the criterion could become a catch-all for numerous cases, undermining the stricter requirements applied to the other two security flag criteria. The introduction of the security flag faced significant criticism during the legislative process[1918], highlighting that the evidentiary hurdle for its application should not be set too low.

7. Remedies against Specific Acts under the Eurodac Regulation

As examined in detail in the preceding chapters, data subjects have a right of access to, rectification, and erasure of data in Eurodac, including Eurodac hits and security flags. Nevertheless, in the view of this study, the Eurodac and Interoperability Regulations do not provide an effective

1918 cf e.g., D1736 from Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (n 298); Access Now, International, AsyLex, Switzerland and Amnesty International, 'Fundamental Rights Concerns about the EURODAC Reform' (8 September 2021) <https://www.statewatch.org/media/2714/eu-eurodac-open-letter-rights-8-9-21.pdf>; Vavoula, 'Focus on Eurodac: Disentangled from the "Package Approach" but Is It Fit to Fly?' (n 607) 19; 'Warnings against Arbitrariness and Mass Surveillance in EURODAC' (*European Digital Rights (EDRi)*, 30 November 2022) <https://edri.org/our-work/warnings-against-arbitrariness-and-mass-surveillance-in-eurodac/> Amnesty International, 'Open Letter to The Rapporteurs on The EU Artificial Intelligence Regulation (AI Act) to Ensure Protection of Rights of Migrants, Asylum Seekers and Refugees' (26 April 2023) <https://www.amnesty.eu/wp-content/uploads/2023/04/TIGO_IOR_10_2023_3987_Open-letter-to-the-Rapporteurs-on-the-EU-AI-Act-1.pdf>.

remedy to challenge, for example, the refusal to rectify data. Such remedies may exist at the national level and, as discussed above, must permit judicial review and an effective challenge of Eurodac data, at least through an appeal against the final decision. In many cases, this is likely to be an appeal against a negative asylum decision or a transfer decision.[1919]

Within the Eurodac system, there are processes beyond the mere storage and processing of data that also raise questions regarding their contestability. The following section will specifically examine whether a data transfer can be contested under the Eurodac Regulation, whether access to Eurodac data by law enforcement authorities can be blocked or subsequently deemed unlawful, and whether the collection of data by EBCG Agency personnel can be challenged.

a) *Remedy against a Transfer of Data*

aa) Data Transfer to Third Countries

The Interoperability Regulations specify that, except for provisions outlined in the Europol, VIS, EES, and ETIAS Regulations, and the querying of Interpol databases via the ESP in compliance with the GDPR, personal data stored in, processed by, or accessed through the interoperability components must not be transferred or made available to any third country, international organisation, or private entity.[1920] Hence, they do not provide grounds for transferring Eurodac data to third countires.

Eurodac data may be shared in accordance with the Eurodac Regulation. Transfers to third countries are permitted in specific circumstances. Eurodac data that are exchanged between Member States following a hit obtained for law enforcement purposes can be transferred to third countries, if there is no "real risk" that, as a result of such transfer, the data subject may be subjected to torture, inhuman and degrading treatment, or any other violation of their fundamental rights.[1921] The same applies for

1919 cf e.g., Asylum Procedure Regulation, Art 67; Return Directive, Art 13. If an exclusion from protection status or a return order is decided on the basis of security concerns, this decision can be appealed.

1920 Interoperability Regulation - Judicial Cooperation, Art 50; Interoperability Regulation - Borders, Art 50.

1921 Eurodac Regulation 2024, Art 49(2) *e contrario*.

personal data that are exchanged between Member States and Europol.[1922] The restriction of this safeguard to data exchanged following a hit has been criticised for creating a significant gap in data protection.[1923]

Furthermore, Eurodac data can be transferred to third countries for the purpose of return, where the Member State of origin agrees and the following two conditions are fulfilled: first, the data are transferred or made available solely for the purpose of identifying an irregularly staying third-country national and issuing an identification or travel document for the purpose of their return. Second, the third-country national concerned has been informed that their personal data may be shared with the authorities of a third country.[1924] The 2016 Eurodac Proposal included additional security measures that were ultimately removed in the final Regulation. Under that proposal, third countries would have been required to explicitly commit to using the data solely for the purpose for which they were provided and to delete them once their retention was no longer justified.[1925] The Eurodac Regulation only holds that data transfers for the purpose of return have to be carried out in accordance with the GDPR.[1926] What follows from this has been discussed in the previous chapters.

Data can finally be transferred if the conditions of Chapter V of the GDPR are observed,[1927] that is when an adequacy decision has been taken[1928] or appropriate safeguards put in place,[1929] unless a specific situation calls for a derogation of said rules.[1930]

In any case, the fact that an application for international protection has been made in a Member State or that a person has been subject to an admission procedure in a Member State must not be disclosed to any third

1922 ibid, Art 49(3) *e contrario*.
1923 FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674), 28; see also FRA, 'The Impact of the Proposal for a Revised Eurodac Regulation on Fundamental Rights: Opinion of the European Union Agency for Fundamental Rights' (n 930).
1924 ibid, Art 50(3).
1925 2016 Eurodac Proposal, Art 38(1)(b).
1926 Eurodac Regulation 2024, Art 50(2).
1927 ibid, Art 49(5).
1928 GDPR, Art 45.
1929 ibid, Art 46.
1930 ibid, Art 49.

country.[1931] Data transfers must not jeopardise the rights of data subjects, particularly with respect to the principle of non-refoulement.[1932]

It should be added that the wider the circulation of data, the greater the risk of data-protection breaches. Civil society organisations have, for instance, reported that Bulgaria shared all fingerprints of asylum seekers claiming to be Syrians with the Consular Section of the Syrian Embassy, putting the concerned individuals at risk.[1933] The ECtHR has likewise recognised that sharing asylum seekers' data with third countries for return purposes may endanger their safety and rights.[1934] The risk extends beyond transfers to third countries: increased data sharing within the interoperable architecture also facilitates the possibility of unlawful access to Eurodac data as the number of access points continues to expand. Where terminals are located in third countries or in facilities hosting third-country liaison officers, the risk of unauthorised access becomes significantly harder to control. This risk is further heightened if interoperable systems can be accessed via mobile devices, which are more vulnerable both to physical interference and to hacking through insecure connections.[1935]

The Eurodac Regulation offers no remedy against the transfer of personal data. If data collected for law enforcement purposes are transferred, the data subject will likely not even be informed about it, leaving them unable to verify whether the transfer conditions are met. In return procedures, individuals likewise may receive no prior notice and are not granted the right to be heard or a remedy in the Eurodac Regulation.[1936]

As mentioned above, data sharing is qualified as a preparatory measure or a 'purely factual act'. The ECJ does not consider it necessary that the

1931 Eurodac Regulation 2024, Art 49(4).

1932 ibid, Art 50(5).

1933 ibid. 27.

1934 In *F.N. and Others v. Sweden*, App no 28774/09 (ECtHR, 18 December 2012) paras 74-76 the ECtHR noted that communication between the authorities of the host country and the consular services of the country of origin for the purpose of return, without explicitly informing that the person has applied for international protection, may give the country of origin sufficient information from which it can be inferred that the person is a rejected asylum seeker.

1935 FRA, 'Fundamental rights and the interoperability of EU information systems: borders and security' (n 674), 26.

1936 This study argues that they will have to be informed if such information will not jeopardies an investigation (see chapter: The Right to Information) and that they need to be informed before a data transfer and have a right to be heard and challenge this decision (see chapters: The Right to Information, and The Right to Rectify Data).

act of data sharing can be challenged if the final act or decision can be contested.[1937] In the case of a return decision, an appeal can be lodged against the final decision.[1938] When data processed for law-enforcement purposes are shared, it remains unclear whether, in each instance, a final decision will be adopted and communicated to the data subject. A criminal investigation may be closed without the individuals concerned ever being informed that their data are held in a police file. It is therefore argued that data subjects ought to be notified of any transfer of their data once disclosure can no longer jeopardise the investigation.[1939] Still, a retrospective challenge would then only be available where the data subject has suffered harm as a consequence of the transfer and is able to rely on the liability provision in Art. 52 of the Eurodac Regulation.

The ECJ held, in its case Schrems I, that when considering a claim by an individual concerning the transfer of personal data outside the EU, "it is incumbent upon the national supervisory authority to examine the claim with all due diligence",[1940] and that in the light of Art. 47 CFR, a data subject should "have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts".[1941] As

1937 *Hans-Martin Tillack v Commission of the European Communities* (n 1619), para 80.

1938 Return Directive, Art 13.

1939 See chapter: The Right to Information, and The Right to Access Personal Data and Information.

1940 *Schrems v Data Protection Commissioner* (n 175), para 63; With respect to the principle of diligence, the Court recalled in *Staelen* that, 'where an administration is called upon to conduct an inquiry, it is for that administration to conduct it with the greatest possible diligence in order to dispel the doubts which exist and to clarify the situation': Case C-337/15 P *European Ombudsman v Claire Staelen* [2017] OJ C 168/8, para 114; cf also Kotschy, 'Article 77 - Right to Lodge a Complaint with a Supervisory Authority' (n 1627) 1223.

1941 *Schrems v Data Protection Commissioner* (n 175), para 64, further states that "[h]aving regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see to this effect Case C-456/13 P *T & L Sugars Ltd, Sidul Açúcares, Unipessoal Lda v European Commission, French Republic, Council of the European Union* [2015] OJ C 213/6, para 48 and the case law cited)." In para 66 the case continues: "Having regard to the foregoing considerations, the answer to the questions referred is that Data Retention Directive, Art 25(6), read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as: Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issues by the US Department of Commerce

discussed, a judicial remedy only exists with regard to the return decision itself. Data subjects should be able, according to the ECJ, to challenge the transfer of their data in front of the national supervisory authority. Otherwise, an adequate level of protection cannot be guaranteed.[1942] National supervisory authorities have encompassing investigation powers.[1943] They can refer a decision to a court for judicial review.[1944] The Eurodac Regulation stipulates that access, rectification, or erasure requests can only be appealed before national supervisory authorities. Accordingly, data subjects are only informed about their right to appeal and the process for submitting an appeal in relation to access, rectification, and erasure requests. Beyond this, Art. 42 Eurodac Regulation merely requires that data subjects be informed of the general possibility to lodge a complaint with the supervisory authority when their fingerprints are taken. It is unlikely that data subjects without legal representation will know that they can appeal a decision to transfer their data with the national supervisory authority. The effectiveness of even this non-judicial remedy must therefore be questioned. This is particularly concerning given that, as outlined above, data protection in relation to the sharing of information with third countries contains noticeable gaps.

bb) Data Transfer within the Schengen Area

Within the Schengen Area, data entered into Eurodac are stored in both the Central System and the CIR, and are thereby made available to all Member States in accordance with the access rights granted to their respective authorities.[1945] If these access rights are breached – for example, where an authority grants access to another authority or official who is not authorised – the data subject may bring a compensation claim, provided that they

---

[2000] OJ L215/7, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection".

1942 *Schrems v Data Protection Commissioner* (n 175), para 49ff.

1943 GDPR, Art 58.

1944 ibid, Art 58(3).

1945 Eurodac Regulation 2024, Art 3(1) and (2); chapter: The Eurodac Regulation.

have suffered damage.[1946] In practice, however, data subjects will rarely be aware that any unlawful disclosure has occurred.

Eurodac data are also transferred between Member States according to Art. 34 Dublin III Regulation (replaced by Art. 37 AMMR). There are data that are not recorded in Eurodac but are nevertheless exchanged between Member States. One example of this is security-relevant information,[1947] another is health data.[1948] According to Art. 12 Eurodac Regulation, health data are not recorded in Eurodac. However, they are needed, for example, when transferring a person from one Member State to another. Art. 32 Dublin III Regulation (replaced by Art. 39 AMMR) requires the transferring Member State to transmit information on any special need. This may include information on that person's physical health in a common health certificate. Health data must only be shared between health professionals, subject to an obligation of professional secrecy. Data subjects have to consent to a transfer.[1949] In the European Commission's study on the implementation of the Dublin III Regulation, some Member States have reported that health data may be brought to the attention of other authorities, such as social welfare and reception officers, legal representatives, police, and immigration services.[1950] They also reported that health data were transmitted without the consent of the individual.[1951] The latter might, under the new law, not be an issue anymore, since Art. 39(3) AMMR holds that "[t]he lack of consent, including a refusal to consent, shall not constitute an obstacle to the transfer." The principle of purpose limitation, as prescribed in Art. 5(1)(b) GDPR, might still be infringed. A UNHCR study further showed that some Member States do not use the common health certificate when transferring data,[1952] which was confirmed by fieldwork conducted

1946 ibid, Art 40.
1947 AMMR, Art 49.
1948 ibid, Art 50.
1949 ibid, Art 50(2) and (3).
1950 DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (n 695) 64; cf also Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 405.
1951 DG Migration and Home Affairs, 'Evaluation of the Implementation of the Dublin III Regulation' (n 695) 64; cf also Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust' (n 564) 405.
1952 Cravesana and Hennessy, 'Left in Limbo: UNHCR Study on the Implementation of the Dublin III Regulation' (n 1327) 145ff.

at reception facilities and at the IOM Mission in Italy.[1953] Instead, Member States have used an IOM data management infrastructure (Migrant Management and Operational Systems Application) to send and receive health data.[1954] The UNHCR study does not explain whether the requirements of the Dublin III Regulation – exchange only between health professionals and with the explicit consent of the data subject – are otherwise met.

There are other challenges with this type of data exchange, which takes place within the framework of the same procedures as the exchange of Eurodac data, e.g., a transfer, but is not based on the Eurodac Regulation. From the perspective of the data subject, it is unclear which data are exchanged by which means and on what legal basis. Access to a remedy is complicated; the Eurodac Regulation does not apply to all data collected and processed from data subjects in an asylum procedure. Eurodac and health care data are, in many cases, collected at the same time, when the data subject is first registered and interviewed.[1955] Yet, the legal process for correcting or deleting such data is not the same. There is also the question of what happens to security-related data. These can be exchanged under the Eurodac Regulation or AMMR. The question is therefore: on what legal basis would a possible exchange have to be contested? From an access to justice perspective, this complexity is not desirable.

b) *Remedy against Access of Law Enforcement Authorities*

As has been described in the first part of this study, designated authorities of each Member State are allowed to request comparison of data with Eurodac data for the prevention, detection, or investigation of terrorist offences or of other serious criminal offences.[1956] To this end, the designated authorities have to submit a reasoned electronic request to the verifying authority, which shall ensure that the conditions for such a comparison are met.[1957] The verifying authority and the designated authorities may be part

1953 Annalisa Pelizza and Chiara Loschi, 'Telling "More Complex Stories" of European Integration: How a Sociotechnical Perspective Can Help Explain Administrative Continuity in the Common European Asylum System' [2023] Journal of European Public Policy 1, 11.

1954 ibid 12.

1955 cf Screening Regulation which requires preliminary health, vulnerability, identification and security checks; AMMR, Art 17; Asylum Procedure Regulation, Art 27.

1956 Eurodac Regulation 2024, Art 5 and 32.

1957 ibid, Art 32(1).

of the same organisation.[1958] Whenever all the conditions for requesting a comparison are fulfilled, the verifying authority transmits the request for comparison to the National Access Point, which will process it to Eurodac for the purpose of comparison with fingerprint and facial image data.[1959]

Like the designated authorities of Member States, Europol cannot access Eurodac directly. It can do so, however, through a National Access Point by a Member State. Europol's designated authority must submit a reasoned electronic request for the comparison, which is examined by a designated unit acting as Europol's verifying authority.[1960] Processing of information obtained by Europol from a comparison with Eurodac data is furthermore subject to the authorisation of the Member State of origin. Such authorisation must be obtained via the Europol national unit of that Member State.[1961]

There is no remedy against a decision of the verifying authority, whether taken by a Member State or by Europol. Neither data subjects nor the designated authorities, or Europol, may challenge such a decision – it is final. Art- 32–34 Eurodac Regulation likewise impose no duty to provide reasons. Verifying authorities are therefore not required to justify why a request by a designated authority or Europol has been granted or refused. The data subject cannot appeal the decision, and it may not even know the basis upon which it was adopted.

Moreover, the data subject is not aware, at that stage, that a law enforcement authority has even submitted a request for a data comparison. As discussed in the previous chapters, the data subject appears not to have a right to be informed of a hit[1962], nor to access related information[1963], at least for as long as such disclosure may interfere with an ongoing investigation. Even

1958 ibid, Art 6(5).

1959 ibid, Art 32(2); according to ibid, Art 32(4), in "exceptional cases of urgency" where there is a need to "prevent an imminent danger associated with a terrorist offence or other serious criminal offence", the verifying authority can transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority. The authority then only verifies ex-post whether all the conditions for requesting a comparison are fulfilled, including whether an exceptional case of urgency actually existed. Where an ex-post verification determines that the access to Eurodac data was not justified, all the authorities that have accessed such data shall erase the information communicated from Eurodac and shall inform the verifying authority of such erasure.

1960 Eurodac Regulation 2024, Art 8.

1961 ibid, Art 34(4).

1962 See chapter: The Right to Information.

1963 See chapter: The Right to Access Personal Data and Information.

if, as argued in this study, one adopts the view that the data subject must be informed when a comparison by a law enforcement authority results in a hit, any review of the verifying authority's decision would necessarily take place ex post – after the decision has already been implemented through the processing of the comparison.

Once a comparison results in a hit, there is no remedy available against the subsequent use of the data. Law enforcement authorities of Member States may process such data without prior authorisation.[1964] Europol, by contrast, must obtain authorisation from the Member State of origin, and that decision is final.[1965] The provision does not establish any criteria that must be satisfied for Europol to be permitted to further process the data, nor does it require that the data subject be informed.[1966] Because the authorisation is granted without substantive conditions, there is no mechanism to verify retrospectively whether it was issued legitimately, rendering the procedure largely formalistic.

In the vast majority of cases, a data subject will only become aware that their data have been cross-checked with Eurodac if they are contacted by the police or public prosecutor in the context of criminal proceedings, whether for questioning or because proceedings have been initiated against them. This raises the question of whether, under national criminal law, a request could be made to disregard the Eurodac hit on the basis of inadmissible evidence. Such a request would entail arguing that the conditions for access set out in Art. 33 or 34 Eurodac Regulation were not fulfilled. It remains unclear whether a national criminal court possesses the authority to assess whether the verifying authority has correctly applied these access requirements under the Eurodac Regulation. Moreover, the consequences of such an assessment are equally uncertain.

The situation may differ if the data subject contends that, although access to the data was legally valid, the hit itself was false or the data stored in Eurodac were inaccurate. In the latter scenario, the individual may request rectification of the Eurodac data pursuant to Art. 43 Eurodac Regulation. If granted, such rectification would be binding on all authorities that have accessed the Eurodac data, in accordance with the principle of data accuracy.[1967] Where the hit itself is inaccurate and this goes undetected –

1964 Eurodac Regulation 2024, Art 32(4); cf also Eurodac Regulation 603/2013, Art 21.
1965 Eurodac Regulation 2024, Art 22(4).
1966 ibid, Art 22(4).
1967 GDPR, Art 5(1)(d); Police Directive, Recital 30.

resulting, for example, in a misidentification – this may also need to be addressed within the context of criminal proceedings. As discussed above, a Eurodac hit constitutes probative evidence in asylum procedures; whether it amounts to formal proof in criminal proceedings remains unclear. Generally, the standard of proof is higher in criminal proceedings than in administrative ones.[1968] A criminal authority may, however, have recourse to an administrative assistance procedure with the relevant Member State authority to clarify the accuracy of a Eurodac hit.[1969]

According to eu-LISA, in 2022, a total of 1,491 data sets were transmitted by Member States' law enforcement authorities for Eurodac comparison, three times as many as the year before.[1970] This produced 30 Category 4 hits.[1971] Europol performed an additional 53 searches in Eurodac, more than double the year before.[1972] The number of hits these produced has not been provided by eu-LISA. The agency also does not publish numbers on how many access requests by law enforcement authorities were rejected.

c) *Remedy against Decisions with Help of EUAA and EBCG Agency Officers*

The Eurodac Regulation allows EBCG Agency and EUAA Member State experts to take fingerprints.[1973] At the discretion of a Member State, the EBCG Agency and Member State's asylum experts, who are deployed to a Member

1968 cf Paul Craig, *EU Administrative Law* (3rd edn, Oxford University Press 2018) 470 ff.

1969 No general rules exist in EU law concerning mutual assistance. The obligation to adhere to the principle of sincere cooperation pursuant to TEU, Art 4(3), may positively influence the interpretation of such sector-specific rules on mutual assistance in secondary law, but most commentators are reluctant to deduce concrete obligations for mutual assistance directly from this primary law provision, according to Schneider, 'Information Exchange and Its Problems' (n 1675) 87 referring to Christoph Ohler, 'Europäisches und Nationales Verwaltungsrecht' in Jörg Philipp Terhechte (ed), *Verwaltungsrecht der Europäischen Union* (2nd edn, Nomos 2022), 9 para 31. Thus, legal gaps exist which are covered only by the application of conventions of the Council of Europe, according to Paul Stelkens, Heinz Joachim Bonk and Michael Sachs, *Verwaltungsverfahrensgesetz: Kommentar* (CH Beck 2014), para 188. Unfortunately, the relevant rules in secondary law are also quite diverse and establish different concepts of mutual assistance, as Schneider, 'Information Exchange and Its Problems' (n 1675) 87ff stipulates.

1970 eu-LISA, 'Eurodac 2022 Annual Report' (n 1194) 17ff.

1971 ibid 22.

1972 ibid 15 and 17.

1973 Eurodac Regulation 2024, Art 15(3), 22(8), 24(8) and 26(5).

State under the auspices of EUAA, can take and transmit fingerprints to Eurodac on behalf of that Member State. The law limits these functions to areas where both agencies' mandates permit them to do this,[1974] for instance, at the external border for persons entering illegally and for asylum applicants.[1975]

The question arises as to which legal remedies and procedural channels are available to data subjects if asylum experts of the EBCG Agency or the EUAA violate their rights or exceed their competences. Art. 52 Eurodac Regulation, which establishes liability, refers explicitly to Member States but makes no mention of the EBCG Agency or the EUAA. These agencies therefore do not appear to be considered data controllers in relation to Eurodac data.[1976] This raises a further question: can the actions and liability of EBCG Agency and EUAA asylum experts be attributed, for liability purposes, to the Member States that deployed them?

The liability provision in Art. 52 Eurodac Regulation only refers to Member States but not to EBCG Agency and EUAA. These, so it seems, are not considered controllers with regard to Eurodac data. Thus, can EBCG Agency and EUAA asylum experts, with regard to liability, be attributed to the Member States that sent them?

Art. 26(1) EUAA Regulation stipulates that civil liability for any damage caused by experts participating in an asylum support team during operations in the host Member State lies with the host Member State, in accor-

1974 cf Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010 [2021] OJ L486/1.
(EUAA Regulation), Art 21 and 32; Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L295/1 (EBCG Regulation 2019), Art 10, 40, 55.

1975 2020 Eurodac Proposal, Explanatory Memorandum 15.

1976 The fact that the role of the two agencies is not clearly defined has been criticised by the EDPS: 'Opinion 9/2020 - EDPS Opinion on the New Pact on Migration and Asylum' (2020), para 10; EDPS, 'Opinion 07/2016 on the First Reform Package on the Common European Asylum System (Eurodac, EASO and Dublin Regulations)' (2016), para 60; and ECRE: 'ECRE Comments on the Commission Proposal for a Screening Regulation COM(2020)612' (n 10) 40; In operations, such as screening and return operations, the Member State and EBCG Agency are considered joint controllers according to: EDPS, 'Audit Report on the European Border and Coast Guard Agency (Frontex)' (2022) Case No. 2022-0749. For a critical lens on these mandates see Michalis Moutselos, 'Expansion without Mandates: Border and Asylum Agencies in European Union Migration Governance' [2024] Governance.

dance with its national law. In cases where the damage results from gross negligence or wilful misconduct by the experts, the host Member State may request reimbursement from the home Member State or the Agency.[1977] Regarding criminal liability, Art. 27 EUAA Regulation states that "[d]uring the deployment of an asylum support team, the deployed experts shall be treated in the same way as officials of the host Member State with regard to any criminal offences that might be committed against them or by them." Apart from proceedings for damages, legal remedies against the agency or its agents are highly limited.[1978]

As an EU agency, EUAA (and the EBCG Agency for that matter) can be investigated under the mandate of the European Ombudsman.[1979] In April 2017, the European Centre for Constitutional and Human Rights called for an inquiry into EASO's involvement in inadmissibility decisions during its mandate in the Greek hotspots. EASO, now known as the EUAA, was scrutinised for its role in these procedures during that time.[1980] Although the Ombudsman "accept[ed] that there [were] genuine concerns about the quality of the admissibility interviews as well as about the procedural fairness of how they [were] conducted", they closed the inquiry into EASO.[1981] In another case, regarding an individual case of an asylum seeker, the Ombudsman considered EASO's failure to address serious errors in asylum procedures it was involved in, to constitute maladministration.

1977 EUAA Regulation, Art 36(1); cf also EBCG Regulation 2019, Art 55.

1978 EUAA Regulation, Art 66, states that: "1. The Agency's contractual liability shall be governed by the law applicable to the contract in question. 2. The CJEU shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency. 3. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties. 4. The CJEU shall have jurisdiction in disputes over compensation for damages referred to in paragraph 3. 5. The personal liability of the Agency's staff towards it shall be governed by the provisions of the Staff Regulations or Conditions of Employment applicable to them."

1979 ibid, Art 67 in conjunction with TFEU, Art 228.

1980 cf European Center for Constitutional and Human Rights, 'Case Report - EASO's Influence on Inadmissibility Decisions Exceeds the Agency's Competence and Disregards Fun-Damental Rights' (2017).

1981 Case 735/2017/MDC *on the European Asylum Support Office's' (EASO) involvement in the decision-making process concerning admissibility of applications for international protection submitted in the Greek Hotspots, in particular shortcomings in admissibility interviews* [2018], Decision of the European Ombusdman, para 46.

Unfortunately, this could not be remedied.[1982] Under the new EUAA Regulation, a complaint mechanism was introduced, offering any person who is directly affected by the actions of an expert participating in an asylum support team, and who considers that their fundamental rights have been violated due to those actions, to submit a complaint in writing to the Agency.[1983] The fundamental rights officer is responsible for handling complaints received by the EUAA.[1984] They can take "appropriate" follow-up measures, including disciplinary measures, or refer the case to a national authority or body.[1985] Whenever an expert is found to have violated fundamental rights or international protection obligations, they can be removed from the activities of the Agency.[1986] Whether the individual complaint mechanism is effective is yet to be seen.

Liability for EBCG team members is regulated in the same manner as for EUAA experts. Art. 84(1) and (2) EBCG Regulation state that, when team members operate in a host Member State, civil liability for any damage caused during their operations lies with the host Member State, in accordance with its national law. In case of gross negligence or wilful misconduct, the home Member State or the Agency can be asked to reimburse paid sums. According to Art. 85 EBCG Regulation, members of the teams in the territory of the host Member State shall be treated in the same way as officials of the host Member State with regard to any criminal offence.[1987]

1982 Case 1139/2018/MDC *on the conduct of experts in interviews with asylum seekers, organised by the European Asylum Support Office* [2019], Decision of the European Ombusdman, para 18; cf also European Asylum Support Office (EASO), 'European Asylum Support Office (EASO) Accepts Ombudsman's Suggestions on How It Reacts to Problems Concerning Interviews with Asylum Seekers' (2020).

1983 EUAA Regulation, Art 51.

1984 ibid, Art 51(4).

1985 ibid, Art 51(5)-(8).

1986 ibid, Art 51(9).

1987 There are special regulations for statutory staff in EBCG Regulation 2019, Art 95; Furthermore, according to EBCG Regulation 2019, Art 96, Protocol No 7 on the Privileges and Immunities of the European Union annexed to the TEU and to the TFEU shall apply to the Agency and its statutory staff: "1. Without prejudice to Articles 84 and 85, the Agency shall be liable for any activities it has undertaken in accordance with this Regulation. 2.The contractual liability of the Agency shall be governed by the law applicable to the contract in question. 3. The Court of Justice shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency. 4. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties, including those related to the

The EBCG's activities are also subject to the inquiries of the European Ombudsman.[1988] Finally, the EBCG Regulation also contains a complaint mechanism in Art. 111. This mechanism enables individuals directly affected by actions or omissions of EBCG staff to submit a complaint, which is subsequently reviewed by the Fundamental Rights Officer.

When EUAA and EBCG experts operate under the Eurodac Regulation, they are bound by its provisions and may only use the collected fingerprints in accordance with the specific purposes outlined in the regulation.[1989] This is particularly crucial in the case of the EBCG, which exercises extensive powers.[1990] Individual complaint mechanisms provide an additional avenue to hold the agencies accountable, a need underscored by the historical lack of accountability of both agencies.[1991] The effectiveness of these mechanisms, however, remains to be assessed.

---

use of executive powers. 5. The Court of Justice shall have jurisdiction in disputes relating to compensation for the damage referred to in paragraph 4. 6.The personal liability of statutory staff towards the Agency shall be governed by the provisions laid down in the Staff Regulations and Conditions of Employment applicable to them"; according to EBCGR Regulation, Art 98, Proceedings may be brought before the Court of Justice for the annulment of acts of the Agency that are intended to produce legal effects vis-à-vis third parties, in accordance with TFEU, Art 263, and for failure to act, in accordance with TFEU, Art 365, for non-contractual liability for damages caused by the Agency and, pursuant to an arbitration clause, contractual liability for damages caused by acts of the Agency, in accordance with TFEU, Art 340."

1988 EBCG Regulation 2019, Art 119; in accordance with TFEU, Art 228.

1989 EUAA Regulation, Art 4(2) and EBCG Regulation 2019, Art 12(1), which state that in order to perform the tasks conferred on them they can, in accordance with these Regulations and other relevant Union and national law regarding the exchange of information, share in a timely and accurate manner all necessary information, does not apply to the deployed experts. In other operations however, such as screening and return operations, the Member State and Frontex are considered joint controllers by the EDPS, as seen above in fn 1976.

1990 cf Luisa Marin, 'The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions' (2020) 26 European Public Law 157.

1991 cf Lena Karamanidou and Bernd Kasparek, *Fundamental Rights, Accountability and Transparency in European Governance of Migration: The Case of the European Border and Coast Guard Agency Frontex* (RESPOND 2020); Evangelia (Lilian) Tsourdi, 'Holding the European Asylum Support Office Accountable for Its Role in Asylum Decision-Making: Mission Impossible?' (2020) 21 German Law Journal 506; Mariolina Eliantonio and Lisi Gaia, 'The Gaps in Judicial Accountability of EASO in the Processing of Asylum Requests in Hotspots' (2019) 4 European Papers - A Journal on Law and Integration 589.

8. Conclusions

The examination of judicial remedies under the Eurodac and Interoperability Regulations reveals a complex landscape, shaped by the intersection of data protection, procedural principles, and practical challenges in cross-border governance. The analysis highlights persistent difficulties in safeguarding data subjects' (procedural) rights and ensuring the availability of effective remedies across Member States.

Direct judicial remedies under the Eurodac and Interoperability Regulations are limited to claims for compensation. These remedies often fall short of addressing the core needs of data subjects, such as access to asylum or other forms of legal status permitting residence in a Member State. Moreover, the requirement to demonstrate direct harm, coupled, potentially, with the complexities of cross-border jurisdiction, frequently undermines both the accessibility and effectiveness of these remedies.

By contrast, indirect judicial review mechanisms within national asylum and migration procedures provide additional avenues for addressing data-related grievances. Although these procedures are not specifically designed to address data protection concerns, they offer a potential means for individuals to challenge administrative decisions that impact their rights under the interoperable Eurodac system. Nevertheless, cross-border obstacles and questions of reviewability may also arise in this context, and the quality and effectiveness of judicial scrutiny vary across Member States.

With regard to extrajudicial review, it is important to note that, while national supervisory authorities play a crucial role in overseeing compliance and addressing complaints concerning data rights, they do not constitute an effective remedy within the meaning of Art. 47 CFR. Despite their powers to investigate and issue binding decisions, such authorities lack the essential characteristics of a 'tribunal' capable of judicial review under EU law; a limitation reinforced by the absence of suspensive effects or guarantees of legal aid in proceedings before them. Furthermore, the study demonstrated a need for procedural coherence and harmonisation across Member States.

The operational complexities and multi-jurisdictional nature of interoperable systems like Eurodac pose significant challenges to transparency and accountability. This complexity often obscures responsibility and hinders effective judicial oversight, complicating the enforcement of rights for data subjects. Variation in procedural standards across Member States and ambiguity in EU case law as well as practice, particularly concerning the

reviewability of acts by foreign authorities, create disparities and uncertainties in the protection of individual rights. Despite these challenges, foundational principles (such as the duty of care and the right to be heard) provide essential safeguards. Still, the analysis shows a need to ensure procedural fairness throughout decision-making processes.

While mutual trust is a cornerstone of EU cooperation, exceptions arise where systemic, and in certain cases individual, deficiencies may give rise to potential violations of fundamental rights, thereby necessitating closer scrutiny. This balance underscores the ongoing need for rigorous examination and potential exceptions to mutual trust in specific circumstances. As this study demonstrates, the principle of mutual trust may at times be interpreted too broadly. The principle should more frequently and rigorously be examined to ensure the effective enforcement of the right to an effective legal remedy.

While Member States enjoy a degree of procedural autonomy, they are bound by EU law to uphold stringent standards of procedural fairness, data accuracy, and respect for privacy rights. The evolution of Eurodac from a fingerprint-based system to an encompassing biometric and biographic database highlights the need for legal frameworks capable of addressing technological advancements, without compromising individual rights. The CJEU emphasises the necessity of thorough judicial review, particularly in asylum cases; it underscores the importance of robust procedural safeguards and the examination of all relevant evidence. A thorough review must also be conducted when biometric data are decisive for a decision. Moreover, it may be necessary in the future to clarify standards of proof to ensure fairness in data processing operations involving biometric data. This should take into account the circumstances under which the data were collected, as well as the often limited access to legal aid and information available to data subjects.

Overall, the evolving challenges in data protection, particularly with the expansion of biometric and biographic data collection under interoperable systems like Eurodac, demand ongoing refinement of legal frameworks and a heightened focus on procedural fairness and access to justice. Strengthening accountability, and the availability of remedies within Eurodac and the Interoperability systems requires dedicated efforts to bolster procedural safeguards and ensure effective judicial oversight. This entails clarifying the scope of judicial competence, strengthening avenues for remedy, ensuring

equal procedural rights, scrutinising the application of mutual trust, and reinforcing instruments that facilitate access to justice.