C. Eurodac and Interoperability

I. The European Union's Interoperable Information Systems

As already mentioned in the introduction, this study deals with Eurodac. However, it is important to understand, especially in the context of interoperability, that Eurodac forms part of a complex network of centralised Europe-wide information systems established in the EU Area of Freedom, Security and Justice (AFSJ), collecting and processing data not only from asylum seekers but also tourists and other migrants. This cluster comprises six information systems. Three are already operational – namely, the Schengen Information System (SIS), Visa Information System (VIS) and Eurodac – and three are forthcoming – the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), as well as the European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN). These databases serve a number of often overlapping purposes, ranging from border management, tackling irregular migration, facilitating returns and law enforcement.[251] Furthermore, in the framework of interoperability, information systems will communicate with each other, enabling the aggregation of personal data from different sources.[252] This dialogue between information systems is facilitated by functions of interoperability, which allow for simultaneous searches in multiple information systems, automatic comparisons of biometric data (fingerprints and facial images) from several information systems, or automatic checking whether the biographical and/or biometric identity data contained in a search exists in other information systems. As part of this development, the older databases, SIS, VIS, and Eurodac were expanded. Eurodac was made into a comprehensive biometric and biographic database, providing access for various purposes, among them law enforcement.

---

251 For an overview of the functioning and interconnection of these databases see Vavoula, *Immigration and Privacy in the Law of the European Union* (n 4).

252 cf High-Level Expert Group on Information Systems and Interoperability, 'High-Level Expert Group on Information Systems and Interoperability (HLEG): Final Report' (European Commission, Directorate-General for Migration and Home Affairs 2017) Ref. Ares(2017)2412067.

It should be recognised that the introduction of this enormous, interconnected data system was viewed critically by many privacy and data security experts. To illustrate this, a quote from a 2010 European Commission paper proves revealing: "A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitute a gross and illegitimate restriction of individuals' right to privacy and data protection and pose huge challenges in terms of development and operation. In practice, policies in the area of freedom, security and justice have developed in an incremental manner, yielding a number of information systems and instruments of varying size, scope and purpose. The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative."[253] The fact that what seemed so unthinkable a decade ago has now been introduced shows that this is a daring endeavour, one might say, in terms of human rights. Only time will tell what the introduction of interoperability really means for the privacy and data protection of those affected. When we discuss Eurodac in this study, it must therefore always be understood that this system works within a connected network of information systems and not as a detached database serving the Dublin system.

II. Eurodac

1. Remodelling Eurodac as a Comprehensive Biometric and Biographic Information System

Eurodac, which means European Dactyloscopy, was introduced in 2003.[254] It was the first biometrically enabled system commissioned by the European Union and the first multinational biometric system globally.[255] The idea of a pan-European fingerprint database arose shortly after the Dublin Convention of 1990 was introduced, which stated that asylum applications

253 'Communication from the Commission to the European Parliament and the Council of 20 July 2010 – Overview of Information Management in the Area of Freedom, Security and Justice' (n 52).
254 Eurodac Regulation 2725/2000.
255 'Eurodac: The European Union's First Multinational Biometric System' (n 6).

should be made in the first country of entry into the European Union.[256] Eurodac was, from the beginning, intrinsically linked to the operation of the Dublin system, which provided allocation mechanisms to identify the Member State responsible for examining an asylum claim through an array of hierarchical criteria.[257] The basic principles underpinning the Dublin system remain in place until today, albeit three times amended. The Convention was replaced by the Dublin II Regulation in 2003,[258] which included certain additions and amendments to the responsibility rules. The Dublin III Regulation was adopted in 2013[259] and will be replaced by the AMMR, the Asylum and Migration Management Regulation, which was adopted in 2024.[260] Eurodac was developed at the same pace. It became operational in 2003 and was amended in the recast Eurodac Regulation 603/2013 adopted in 2013. Up until recently, Eurodac stored ten rolled fingerprints, the data subject's gender, and a reference number as well as the state sending the data and the place and date of the international protection application (if applicable).[261] It collected these data from asylum seekers and third-country nationals or stateless persons apprehended in connection with the irregular crossing by land, sea or air of the border of a Member State.[262] Eurodac was a relatively limited biometric database focused on asylum allocation. This has changed considerably.

256 Convention Determining the State Responsible for Examining Applications for Asylum Lodged in One of the Member States of the European Communities [1997] OJ C254/01 (Dublin Convention), Art 3(2).

257 ibid.

258 Council Regulation (EC) No 343/2003 of 18 February 2003 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 [2003] OJ L50/1 (Dublin II Regulation).

259 Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 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).

260 See chapter: Introduction.

261 Eurodac Regulation 2000, Art 5(1), 8(2); Regulation on the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin III Regulation [2013] OJ L180/1 (Eurodac Regulation 603/2013).

262 Eurodac Regulation 2000, Art 4(1), 8(1); Eurodac Regulation 603/2013, Art 9(1), 14(1).

Since 1999, the EU has aimed to create the CEAS,[263] harmonising many aspects of the asylum system in the EU Member States. As a result, directives and regulations have been issued that regulate various aspects of asylum procedures and reception conditions throughout the EU. The centrepiece of the CEAS was the Dublin III Regulation, which embodies the principle of negative mutual recognition and the introduction of automaticity among Member States; where one of the Dublin criteria is met, the responsible Member State recognises the refusal of another Member State to examine the asylum application, and an automatic transfer.[264] Major changes have been underway in the last years.[265] On 4 May 2016, the Commission adopted the 2016 Eurodac Proposal[266] in the framework of revising the CEAS-related legal instruments.[267] The proposal effectively separated Eurodac from its asylum framework and rebranded it as a system aimed at "wider immigration purposes"[268] with a significant emphasis on internal

263 On the principle of solidarity in the EU AFSI, see Treaty on the Functioning of the European Union [1975] OJ C202/1 (TFEU), Art 80.

264 Elspeth Guild, 'Seeking Asylum: Storm Clouds between International Commitments and EU Legislative Measures' (2004) 29 European Law Review 198.

265 Vavoula, 'Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration' (n 12) 3ff.

266 Proposal for a Regulation on the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of Dublin III Regulation (recast) [2016] COM(2016)272 (2016 Eurodac Proposal).

267 Proposal for a 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 Stateless Person (recast) [2016] COM(2016)270 (Proposal for Dublin Regulation 2016); Proposal for a Regulation on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, for a Uniform Status for Refugees or for Persons Eligible for Subsidiary Protection and for the Content of the Protection Granted [2016] COM(2016)466 (Proposal International Protection Standards Regulation); Proposal for a Regulation Establishing a Common Procedure for International Protection in the Union [2016] COM(2016)467 (Proposal for Asylum Procedures Regulation); Proposal for a Directive Laying down Standards for the Reception of Applicants for International Protection (recast) [2016] COM(2016)465 (Proposal for Reception Standards Directive); Proposal for a Regulation on the European Union Agency for Asylum [2016] COM(2016)271 (Proposal EUAA Regulation); Proposal for a Regulation establishing a Union Resettlement Framework [2016] COM(2016)468 (Proposal for a Regulation Union Resettlement Framework).

268 2016 Eurodac Proposal 6.

security.[269] The negotiations on that proposal led to an interinstitutional agreement in mid-2018 between the co-legislators. On 23 September 2020, the Commission proposed further amendments to the Eurodac system[270] within the framework of the New Pact on Migration and Asylum. The amended proposal prescribes several amendments to the functionalities of Eurodac both in the framework of CEAS and migration control as well as in an interoperable environment, whilst taking into account the 2018 interinstitutional agreement between the Council and the Parliament. Finally, on 14 May 2024, the EU Pact on Migration and Asylum was adopted by the European Council, and with it the reformed Eurodac Regulation.[271] As will be seen in the next section, the new Eurodac is a comprehensive biometric and biographic database. It stores data from a wide range of categories of asylum seekers and irregularly staying or entering third-country nationals, including children from the age of 6. It provides access for law enforcement authorities and Europol and uses the huge volume of data to evaluate migration flows, behavioural patterns and movements of migrants.

2. Eurodac Regulation (EU) 2024/1358

a) *Legal Basis and Purpose*

The legal foundation for Eurodac is provided by Regulation (EU) 2024/1358, which establishes Eurodac for the comparison of biometric data. This regulation aims to effectively implement the Asylum and Migration Management Regulation (AMMR), the regulation establishing a Union Resettlement and Humanitarian Admission Framework, and the Temporary Protection Directive. It also facilitates the identification of illegally residing third-country nationals and stateless persons and allows Member States' law enforcement authorities and Europol to request comparisons with Eurodac data for law enforcement purposes. Additionally, this regulation amends the ETIAS and Interoperability Regulations while repealing the previous Eurodac Regulation.

269 E.g., ibid 5.

270 2020 Eurodac Proposal.

271 'The Council Adopts the EU's Pact on Migration and Asylum' (*Council of the European Union*, 14 May 2024) <https://www.consilium.europa.eu/en/press/press-releases/2024/05/14/the-council-adopts-the-eu-s-pact-on-migration-and-asylum/>.

As already mentioned, the purpose of the regulation has been massively expanded compared to the old Eurodac Regulation. Eurodac is now not only a comprehensive biometric and biographical database. It also serves law enforcement purposes in addition to asylum law objectives. A total of ten purposes are listed in the regulation. In addition to supporting the asylum system and assisting with the application of the AMMR, the database assists with the control of irregular immigration to the Union, the detection of secondary movement, and illegally staying persons.[272] The regulation defines the conditions for law enforcement access to Eurodac[273] and assists in the identification of persons by police authorities for identification.[274] The database also assists with the protection of children, including in the context of law enforcement.[275] An additional new function of the database is its 'interoperability', which means that Eurodac supports ETIAS and VIS objectives.[276] Furthermore, comprehensive data collection from all persons wishing to travel to the EU will feed statistics used by different EU bodies, among them the border guards and the European Border and Coast Guard (EBCG), also known as Frontex. [277] Finally, Eurodac assists with the implementation of the Temporary Protection Directive.[278]

b) *Affected Persons*

The Eurodac Regulation applies to third-country nationals and stateless persons, who are divided into different categories: applicants for international protection,[279] persons registered for the purpose of conducting an admission procedure under the Union Resettlement and Humanitarian Admission Framework,[280] persons admitted in accordance with a national resettlement scheme,[281] third-country nationals or stateless persons apprehended in connection with the irregular crossing of an external border,[282]

272 ibid, Art 1(1).
273 ibid, Art 1(1)(e).
274 ibid, Art 1(1)(f).
275 ibid, Art 1(1)(d).
276 ibid, Art 1(1)(g), (h).
277 ibid, Art 1(1)(i).
278 ibid, Art 1(1)(j).
279 ibid, Art 15.
280 ibid, Art 18.
281 ibid, Art 20.
282 ibid, Art 22.

illegally staying in a Member State,[283] or disembarked following a search and rescue operation[284] (SAR),[285] and beneficiaries of temporary protection.[286] The categorisation of persons seeking international protection into different categories was controversial during the legislative process. The ECJ recalls in the case Cimade and Gisti that EU law views asylum seeker status – at least with regard to reception conditions – as a single, indivisible class of protected persons.[287] The category of data subjects disembarked following a search and rescue operation attracted particular criticism, as it may mark the beginning of differentiated treatment for this group.[288] The EU wanted to collect statistics on this category of data subjects.[289]

For all these categories, data are taken from adults and children from the age of six years.[290] An exception is only made when a third-country national or stateless person apprehended in connection with the irregular crossing of an external border is turned back immediately or is detained during the entirety of the period between their apprehension and removal.[291]

Territorially, the Regulation is applicable only to territory to which the AMMR[292] applies, with the exception of the provisions related to data

283 ibid, Art 23.
284 ibid, Art 24.
285 SAR is defined as operations of search and rescue as per the International Convention on Maritime Search and Rescue [1985] 23489.
286 Eurodac Regulation 2024, Art 26.
287 *CIMADE and GISTI v Ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration* (n 183); on the problems of dividing asylum seekers into different categories, with different rights see e.g. Mouzourakis Minos 'More laws, less law: The European Union's New Pact on Migration and Asylum and the fragmentation of "asylum seeker" status' 2020 (26) European Law Journal 171–180.
288 cf e.g., 9103/22 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 - Comments from the Delegations' (18 May 2022), Austria.
289 cf e.g. ibid, Poland.
290 Eurodac Regulation 2024, Art 14, 15, 18, 20, 22, 23, 24.
291 ibid, Art 22(1).
292 ibid, Art 60.

collected to assist with the application of the Resettlement Regulation[293] under the conditions set out in the Eurodac Regulation.[294]

c) *Structure and Procedures*

aa) Components of Eurodac

eu-LISA is responsible for the operational management of Eurodac.[295] It will utilise real personal data from the Eurodac production system for testing purposes, diagnostics, and repairs when faults are identified. This data will also be used to test new technologies and techniques aimed at enhancing Eurodac's performance or the transmission of data to the system.[296] The latter means that eu-LISA will likely be using facial images of asylum seekers to train their facial recognition software, as it "may use real personal data from the Eurodac production system for testing purposes" according to Art. 4(2) Eurodac Regulation. By 2020 eu-LISA was supposed to have conducted a study on the technical feasibility of adding facial recognition software to the Eurodac Central System for the purposes of comparing facial images.[297] This study has, to this day, not been conducted.[298]

Eurodac consists of four components: first, the so-called Central System.[299] This system is composed of a Central Unit along with a Business Continuity Plan and System. Second, Eurodac entails the CIR,[300] which is also at the core of interoperability and stores an individual file for each person registered in any of the underlying systems, such as Eurodac. The other two components are the communication infrastructure between the

293 Regulation (EU) 2024/1350 of the European Parliament and of the Council of 14 May 2024 establishing a Union Resettlement and Humanitarian Admission Framework [2024] (Resettlement Regulation).
294 Eurodac Regulation 2024, Art 60.
295 ibid, Art 4(1).
296 ibid, Art 4(2).
297 2016 Eurodac Proposal, Art 42(4).
298 According to D1736 from Wojciech Wiewiórowski - EDPS, 'EDPS Replies to the Additional Questions on Data Protection in the Proposal for a Recast of Eurodac Regulation' (15 July 2022) 6 the foreseen study will furthermore "focus only on the technical aspects and not on the necessity and proportionality of processing of facial images."
299 Eurodac Regulation 2024, Art 3(1)(a).
300 ibid, Art 3(1)(c).

Central System and Member States,[301] as well as the secure communication infrastructure between the Central System and the central European search portal between the Central System and the CIR.[302] Each Member State and Europol have a single access point, the National Access Point or Europol Access Point respectively.[303]

CIR contains the data that are collected according to Art. 17(1) Eurodac Regulation, with a few exceptions.[304] The remaining Eurodac data is stored in the Central System.[305] Besides fingerprints, facial images, and biographic data, this includes a scanned colour copy of an identity or travel document, operator user ID,[306] where applicable and available information regarding relocation, transfers, removal from territory, or the fact that a person could pose a threat to internal security.[307] Additionally, the Central System and the CIR provide the electronic means to transmit data between Eurodac and the Member States[308] and facilitate comparison with ETIAS.[309]

bb) Taking of Biometric Data

Member States have to impose on all data subjects the requirement to provide their fingerprints and facial image.[310] Biometric data of minors from the age of six must be collected by trained officials and in a child-friendly/child-sensitive manner.[311] From applicants for international protection,

301 ibid, Art 3(1)(b).
302 ibid, Art 3(1)(d). According to ibid, Art. 3(3), the Communication Infrastructure uses the 'Secure Trans European Services for Telematics between Administrations' (TESTA) network. In order to ensure confidentiality, personal data transmitted to or from Eurodac shall be encrypted.
303 ibid, Art 3(4).
304 ibid, Art 3(2) in conjunction with ibid, Art 17, 19, 21, 22, 24 and 26. Exception are the Member State of origin, place and date of the application for international protection, the scanned colour copy of an identity or travel document and the reference number used by the Member State of origin, the reference number used by the Member State of origin, the date on which the biometric data were taken and transmitted to Eurodac and the operator user ID.
305 ibid, Art 3(2) and Art 17.
306 ibid, Art 17(1).
307 ibid, Art 17(2).
308 ibid, Recital 17.
309 ibid, Art 8.
310 ibid, Art 13.
311 ibid, Art 14. The provision states that: "No form of force shall be used against minors to ensure their compliance with the obligation to provide biometric data.

biometric data are taken when they make the application for international protection[312] or when the application[313] or an admission procedure for resettlement[314] or temporary protection[315] is registered. In any other case, fingerprints are taken after the apprehension of the person.[316] If this is requested by the Member State concerned, the biometric data, biographic data and, where available, a scanned colour copy of an identity or travel document may also be taken and transmitted on behalf of that Member State by members of the EBCG or experts of the asylum support teams of European Union Agency for Asylum (EUAA).[317]

National law can foresee administrative measures for the purpose of ensuring compliance with the obligation to provide biometric data, which, according to Art. 13(3) Eurodac Regulation, may include the possibility to use means of coercion as a last resort. Measures should not be employed when a data subject is deemed vulnerable due to the condition of their fingertips or face, provided that this condition was not intentionally caused by the individual.[318] Special provisions also apply to minors, where only as a "last resort, a proportionate degree of coercion" may be used.[319] The use of data for law enforcement purposes is limited for children under the age of 14.[320]

cc) Transmission of Data

After retrieving biometric data, Member States must transmit it to Eurodac no later than 72 hours from the date of registration, apprehension, embarkation, or the date the data were collected or the individual was identified as staying irregularly in a Member State.[321] Only for beneficiaries

---

However, 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 that obligation."

312 ibid, Art 14(1)(b).
313 ibid, Art 14(1)(a).
314 ibid, Art 18 and Art 20.
315 ibid, Art 26.
316 ibid, Art 22-24.
317 ibid, Art 15(3), 22(8), 24(8) and 26(5).
318 ibid, Art 13(5).
319 ibid, Art 14(1).
320 ibid, Art 14(3).
321 ibid, Art 15(1), 18(2), 20(1), 22(2), 23(2) and 24(2).

of temporary protection is there a ten-day time limit.[322] At the same time, all the other data collected is also sent to Eurodac. The Eurodac Regulation uses the term 'Member State of origin' in some of its provisions, which means the Member State that transmits the personal data to Eurodac and, except in resettlement cases, receives the results of the comparison.[323]

Non-compliance with the 72-hour time limit does not relieve Member States of the obligation to take and transmit the biometric data to Eurodac. If the condition of the fingertips does not provide sufficient quality for an accurate comparison, the Member State must retake the fingerprints and resend them as soon as possible, and no later than 48 hours. In cases of resettlement, the fingerprints should be sent as soon as possible after successful retaking.[324]

In the event of serious technical problems, Member States may extend this time by a maximum of a further 48 hours in order to carry out their national continuity plans.[325] In case of further Eurodac-relevant events, e.g., a data subject leaving the territory of a Member State after a return decision or removal order, the data entry must be updated.[326]

Biometric data and other personal data are digitally processed and transmitted. eu-LISA has to establish the technical requirements for transmission of the data format by Member States to Eurodac and vice versa. Further, it must ensure that the biometric data transmitted by the Member States can be compared.[327] Eurodac confirms the receipt of transmitted data as soon as possible.[328]

322 ibid, Art 26(2).
323 ibid, Art 2(1)(e).
324 ibid, Art 15(1), 18(3), 20(2), 22(4), 23(4), 24(4) and 26(3). Also: Where it is not possible to take the biometric data of a person on account of measures taken to ensure his or her health or the protection of public health, Member States take and send such biometric data as soon as possible and no later than 48 hours after those health grounds no longer prevail (ibid, Art 15(1), 18(3), 20(2), 22(4), 23(5), 24(5) and 26(4).
325 ibid, Art 15(2), 22(6), 23(5), 24(5), and 26(4).
326 ibid, Art. 24(7), 16(2)(c), (d), 22(7), 23(6), 24(7) and 26(6).
327 ibid, Art 37(1), (2).
328 ibid, Art 37(6).

dd) Marking of Data

The Member State of origin that granted international protection to an applicant, whose data were previously recorded in Eurodac, has to mark the relevant data.[329] This mark is stored in Eurodac for the purpose of comparison of biometric data.[330] Similarly, data from data subjects who were granted residency documents after staying irregularly in a Member State or who disembarked following a search and rescue (SAR) operation is also marked.[331] Eurodac must inform all Member States of origin about the marking of data by another Member State that produced a hit with the transmitted data as soon as possible and no later than 72 hours. Following this notification, the Member States of origin are required to mark the corresponding data sets.[332] Finally, when a data subject is relocated, the Member State of relocation registers itself as the responsible Member State and marks the data with the designation established by the Member State that granted protection.[333]

Marked data remains available for comparison for law enforcement purposes until it is automatically erased after ten or five years, respectively.[334]

ee) Processing and Comparing of Data

Biometric data transmitted by any Member State to Eurodac are compared automatically with biometric data transmitted by other Member States already stored in Eurodac and, on request, also data transmitted previously by the same Member State[335, 336] A hit, that is, confirmation that a comparison of the data appears to have resulted in a match, or the negative result of the comparison is transmitted to the Member State of origin. In case of a

329 ibid, Art 37(1).
330 ibid, Art 31(1) in conjunction with ibid, Art 27 and 28.
331 ibid, Art 31(4).
332 ibid, Art 31(1), (4).
333 ibid, Art 31(6) and 25.
334 ibid, Art 31(2) in conjunction with ibid, Art 29(1), (2), (8) and (10).
335 ibid, Art 27(3).
336 ibid, Art 27(1), which holds an exception for data according to Art. 16(2)(a)(c) and for data subject in a national or Union resettlement procedure according to Art. 18 and 20 Eurodac Regulation 2024 respectively; for data subjects in Proposal for a Directive Union Resettlement Framework, Art 18, comparisons are still made, but according to Eurodac Regulation 2024, Art. 27(2).

hit, all the data recorded in Eurodac for all corresponding datasets will be sent to the Member State of origin.[337] Member States, not Eurodac, carry out a comparison of facial image data, where the condition of the fingertips does not allow for a comparison of good enough quality.[338] However, facial images and data relating to the sex of a data subject are still compared automatically with corresponding data items stored in Eurodac.[339]
Eurodac links datasets in a sequence when at least one set of fingerprints or, where the quality of the fingerprints does not allow for reliable comparison, the facial image corresponds to the same data subject.[340] This linkage is not confirmed by a fingerprint or facial image expert.

Eurodac has to, as soon as possible, check the quality of the transmitted biometric data. If the biometric data do not lend themselves to comparison using the computerised fingerprint and facial recognition system, the concerned Member States are informed and must resend better quality data.[341] Eurodac processes comparison requests in the order they are received, ensuring that each request is addressed within 24 hours of its arrival. Member States can ask for comparisons to be made in one hour in particularly urgent cases.[342]

Only "where necessary" will a fingerprint expert in the receiving Member State check the result of the comparison of fingerprint data carried out by Eurodac.[343] If Eurodac returns both a fingerprint match and a facial image match after comparing the data with the records in the centralised database, Member States may verify the results of the facial image comparison.[344] Only in cases of hits based just on facial images is the immediate check required by an expert "trained in accordance with national practice" but not national law.[345] If the final identification indicates that the hit was inaccurate, Member States must immediately erase the comparison result

337 Eurodac Regulation 2024, Art 27(4).
338 ibid, Art 28(1).
339 ibid, Art 28(1), with the exception of those transmitted in accordance with Article 16(2), points (a) and (c), and Articles 18 and 20; for data subjects in Proposal for a Regulation Union Resettlement Framework, Art 18, comparisons are still made, but according to Eurodac Regulation 2024, Art. 28(3).
340 Eurodac Regulation 2024, Art 3(6) and Art. 15(4), 22(9), 23(7) and 24(9).
341 ibid, Art 38(1).
342 ibid, Art 38(2).
343 ibid, Art 38(2) in conjunction with ibid, Art 27.
344 ibid, Art 38(4).
345 ibid, Art 38(5).

and notify eu-LISA of this fact as soon as possible, and no later than three working days after receiving the result.[346]

d) *Collection and Storage of Data*

aa) Collection of Data

Eurodac started out as a database primarily for the storage and comparison of fingerprints for the purpose of the implementation of the Dublin system. However, as seen above, the purpose of the database has been broadened considerably and so has the range of data collected. Besides fingerprints and facial images, there is a list of up to 26 data items that are collected from data subjects, if available, and stored in Eurodac. Among them are fingerprints, facial images, nationality, place and date of birth, sex, identity or travel document (including a scanned photocopy along with an indication of its authenticity), information on the responsible Member State, arrival and transfer dates, along with the fact that a visa was issued to the data subject by a Member State, that they might pose a threat to internal security, and asylum-related former decisions.[347] Additional information regarding the status of the data subjects, such as a transfer after a take charge or take-back request, is stored in Eurodac.[348] In order for a data entry to be considered a data set for the purpose of multiple-identity detection according to Art. 27(1)(c) Interoperability Regulation, the following data must be recorded: fingerprint and facial image data, all names (including aliases), nationality(ies), date and place of birth, as well as sex.[349]

bb) Storage and Erasure of Data

Each set of data relating to an applicant for international protection is stored in Eurodac for ten years from the date when biometric data were transmitted.[350] Sets of data relating to other data subjects are stored in

346 ibid, Art 38(6).
347 ibid, Art 17(1), (2).
348 ibid, Art 16.
349 ibid, Art 17(3).
350 ibid, Art 29(1).

Eurodac for five years from the transmission date,[351] with the exception of data subjects in Union resettlement frameworks that are not granted international protection or humanitarian status, whose data are recorded for three years,[352] and beneficiaries of temporary protection, whose data are stored for one year.[353] Upon expiry of the data storage periods, Eurodac automatically has to erase the data.[354]

Only data relating to a person who has acquired citizenship of any Member State before expiry of this period have to be erased from Eurodac. This is as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship. Eurodac shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure.[355]

cc) Keeping of Records

eu-LISA must keep records of all data processing operations within Eurodac. Those records must include the purpose, date and time of access, the data transmitted, the data used for querying, and the name of both the unit entering or retrieving the data and the persons responsible.[356] The agency also has to keep such records for the purposes of interoperability with ETIAS. These records shall additionally show the hits triggered while carrying out automated processing in line with the ETIAS Regulation.[357] 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.[358] The Eurodac Regulation only regulates the erasure of records of data processing operations within Eurodac. The data records must be erased one year after the expiry of the applicable storage period mentioned above, which may be one, three, five, or ten years.

351 ibid, Art 29(3), (5-8).
352 ibid, Art 29(4) in conjunction with ibid, Art 18(2)(b) or (c).
353 ibid, Art 29(9) in conjunction with ibid, Art 26(1).
354 ibid, Art 29(10).
355 ibid, Art 30.
356 ibid, Art 41(1).
357 ibid, Art 41(2); in conjunction with ETIAS Regulation, Art 20.
358 Eurodac Regulation 2024, Art 41(3) in conjunction with Amendment to the VIS Regulation 2021, Art 34.

They can, however, be kept for longer, if they are required for "monitoring procedures which have already begun".[359]

Eurodac, the designated and verifying authorities, and Europol also must keep records of their searches. 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 as well as for preparing annual reports.[360] Other than for such purposes, personal data, along with the records of the searches, must 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.[361]

Finally, each Member State and Europol have to ensure that all data processing operations resulting from requests for comparison with Eurodac data for law enforcement purposes are logged or documented. These records are used for checking the admissibility of the request, monitoring the lawfulness of the data processing and data integrity, as well as for security and self-monitoring.[362] The Eurodac Regulation contains a list of information that must 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, those who ordered and carried it out, as well as the data used for comparison.[363] Logs that contain personal data can be used for monitoring the lawfulness of data processing in combination with data security and integrity. For monitoring and evaluation, only non-personal data may additionally be used.[364]

dd) Statistics

The lengthiest article in the Eurodac Regulation is dedicated to statistics. A total of 23 points and 43 sub-points are listed, which must be reported as statistics, indicating among other things: numbers of every data subject category, the number of hits for each data subject, the number of marked and unmarked datasets, the number of biometrics which, due to quality

359 Eurodac Regulation 2024, Art 41(4).
360 ibid, Art 47(4).
361 ibid, Art 47(4).
362 ibid, Art 51(1).
363 ibid, Art 51(2).
364 ibid, Art 51(3).

issues, had to be requested more than once, the number of requests and hits by designated authorities and Europol, as well as the number of requests under the right to access, rectification, and erasure of data.[365] Every year, eu-LISA publishes the yearly data broken down by Member State. This includes, for the data sets transmitted concerning asylum seekers, individuals crossing an external border or staying irregularly in a Member State, those disembarking following a SAR operation, and persons within Union resettlement frameworks, the year of birth and sex of the data subjects.[366] eu-LISA will also publish monthly cross-system statistics, which are made available to Member States, the European Parliament, the Commission, EUAA, the EBCG and Europol, but not, it seems, to the public.[367] The Commission can request statistics on specific aspects.[368]

e) *Access to Eurodac Data*

aa) Access to Data in the CIR

Access to Eurodac data in the CIR is restricted to authorised personnel from each Member State and the Union who are responsible for identification, such as police authorities. This access is also granted for manual verification of different identities when the Multiple Identity Detector (MID) generates a yellow or red link between data sets.[369]

bb) Access to Data in Eurodac

aaa) *Member States of Origin*

The Member State of origin has access to data they transmitted and that are recorded in Eurodac.[370] Member States are not allowed to conduct searches of the data transmitted by another Member State, nor may they receive such

365 ibid, Art 12(1).
366 ibid, Art 12(2).
367 ibid, Art 12(3).
368 ibid, Art 12(4).
369 ibid, Art 40(4); in conjunction with Interoperability Regulation - Judicial Cooperation, Art 20 and 21.
370 Eurodac Regulation 2024, Art 40(1).

data apart from data resulting from a hit.[371] Also, only Member States of origin are allowed to amend the data they have transmitted, by rectifying, supplementing, or erasing them.[372]

The authorities of Member States with access to data recorded in Eurodac are those designated to assist in determining which Member State is responsible for examining applications for international protection, as well as in controlling irregular migration to the Union and managing temporary protection. Each designation must specify the exact unit responsible for carrying out tasks related to the application of the Eurodac Regulation. Member States must communicate this designation and any amendments to the Commission, which eu-LISA publishes annually in the Official Journal of the European Union.[373]

bbb) *Designated Authorities*

Within Member States, certain authorities are allowed to access Eurodac data for law enforcement purposes, under specific conditions. For this, Member States designate authorities that are authorised to request comparisons with Eurodac. Designated authorities must be authorities who are responsible for the prevention, detection, or investigation of terrorist offences or other serious criminal offences. Each Member State keeps a list of the designated authorities and of the operating units within these authorities.[374]

Furthermore, each Member State must designate a verifying authority, which ensures that conditions for comparison of data with Eurodac for law enforcement purposes are fulfilled.[375] This authority must be an authority responsible for the investigation of terrorist and serious offences in the Member State. It can even be part of the same organisation as the designated authority, as long as they perform their tasks independently.[376] Only the verifying authority is allowed to forward requests for comparison of data to the National Access Point.[377] Requests for comparison with Eurodac data

371 ibid, Art 40(1) in conjunction with ibid, Art 27 and 28.
372 ibid, Art 40(3).
373 ibid, Art 40(2).
374 ibid, Art 5.
375 ibid, Art 6(2).
376 ibid, Art 6(1).
377 ibid, Art 6(2).

are not limited to specific data but can be carried out with biometric or biographic data.[378]

In order to be able to access Eurodac data, the designated authority must submit a reasoned electronic request along with the reference number used by them to the verifying authority. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison are fulfilled.[379] Where all the conditions for requesting a comparison are met, the verifying authority transmits the request for comparison to the National Access Point, which will forward it to Eurodac for the purpose of comparison with biometric or alphanumerical biographic data.[380]

The first condition for designated authorities to access Eurodac is that a search must be conducted in the national databases and the Automated Fingerprint Identification Systems (AFIS) of all other Member States, unless there are reasonable grounds to believe that such a comparison would not lead to the establishment of the data subject's identity.[381] Such grounds must be included in the reasoned electronic request. Designated authorities may also check the VIS.[382] Additionally, the following cumulative conditions have to be met: first, the comparison is necessary for the purpose of the prevention, detection, or investigation of terrorist offences or of other serious criminal offences; there needs to be an overriding public security concern that makes the searching of the database proportionate. Second, the comparison is necessary in a specific case, so no systematic comparisons shall be carried out. Third, there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection, or investigation of any of the criminal offences in question. Such reasonable grounds exist, in particular, where there is a substantiated suspicion that the suspect, perpetrator, or victim of a terrorist offence or other serious criminal offence falls in a category covered by the Eurodac Regulation.[383]

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 biographic or

378 2016 Eurodac Proposal, Art 21(2); 2020 Eurodac Proposal, Art 21(2).
379 Eurodac Regulation 2024, Art 32(1).
380 ibid, Art 32(2).
381 ibid, Art 33(1)(a).
382 ibid, Art 33(1).
383 ibid, Art 33(1)(b), (c).

alphanumerical data to the National Access Point for comparison immediately upon receipt of a request by a designated authority.[384] The authority then only verifies ex post whether all the conditions for a comparison are fulfilled, including whether an exceptional case of urgency actually existed.[385] Whenever an ex post verification determines that the access to Eurodac data was not justified, all the authorities who have accessed such data shall erase the information communicated from Eurodac and shall inform the verifying authority of such an erasure.[386]

A second exception from the aforementioned conditions occurs regarding access to the CIR under the Interoperability Regulation. According to the Interoperability Regulation, designated authorities may check the CIR to determine whether data on a specific individual are present in Eurodac, provided there are reasonable grounds to believe that such consultation will aid in the prevention, detection, or investigation of serious criminal or terrorist offences.[387] If this is the case, designated authorities can access Eurodac without a prior check of national databases or AFIS of other Member States.[388]

ccc) *Europol*

Like the designated authorities, Europol can also access Eurodac data in order to support action by Member States in preventing, detecting, or investigating terrorist offences or other serious criminal offences, if certain conditions are fulfilled. Europol has to designate one or more of its operating units as the 'Europol designated authority'.[389] Europol also designates a single specialised unit to act as its verifying authority, which can forward requests for data comparison to Eurodac through the Europol Access Point. The unit must ensure that the conditions for requesting comparisons of data with Eurodac data are fulfilled.[390] Comparisons of data can be made with biometric or alphanumerical biographic data.[391]

384 ibid, Art 32(4).
385 ibid, Art 32(4).
386 ibid, Art 32(5).
387 Interoperability Regulation - Judicial Cooperation, Art 22.
388 Eurodac Regulation 2024, Art 33(3).
389 ibid, Art 7(1).
390 ibid, Art 7(2).
391 ibid, Art 34(3).

Europol's designated authority must submit a reasoned electronic request for comparisons with data stored in Eurodac. This is only granted if, first, comparison with data stored in any other information processing systems accessible by Europol did not lead to the establishment of the identity of the data subject. Second, the following three cumulative conditions have to be met: the comparison is necessary to support and strengthen action by Member States in preventing, detecting, or investigating terrorist offences or other serious criminal offences falling under Europol's mandate. Thus, in this case, there is an overriding public security concern that makes the searching of the database proportionate. The comparison is necessary in a specific case, meaning that no systematic comparisons shall be carried out. Finally, there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection, or investigation of any of the criminal offences in question. Such reasonable grounds exist, in particular, whenever there is a substantiated suspicion that the suspect, perpetrator, or victim of a terrorist offence or other serious criminal offence falls in a category covered by the Eurodac Regulation.[392]

There is no urgency exception for Europol access to Eurodac data. Nevertheless, the above-mentioned exception after a prior check of the CIR, according to the Interoperability Regulation, also applies for Europol.[393] In that case, Europol can access Eurodac under the aforementioned conditions.[394]

Other than for designated authorities, processing of information obtained by Europol from a comparison with Eurodac data is subject to the authorisation of the Member State of origin. Such authorisation must be obtained via the Europol national unit of that Member State.[395]

ddd) *ETIAS Central System and ETIAS National Unit*

Eurodac data can be accessed by the ETIAS National Unit. Data in Eurodac is automatically compared to ETIAS data, which in this study is considered a form of access. Eurodac is connected to the European Search Portal

392 ibid, Art 34(1).
393 Interoperability Regulation - Judicial Cooperation, Art 22.
394 Eurodac Regulation 2024, Art 33(2).
395 ibid, Art 33(3).

(ESP)[396] in order to enable the automated processing by the ETIAS.[397] The automated processing checks whether the data correspond to any of the events outlined in the ETIAS Regulation.[398] This includes verifying if the travel document used by the data subject matches a document reported lost, stolen, misappropriated, or invalidated in the SIS. It also determines whether the data subject is currently reported as an overstayer or has been reported as such in the past in the EES, and whether the data subject has faced a decision to refuse, annul, or revoke a short-stay visa recorded in the VIS.[399] For the purpose of verifying whether a person is registered in Eurodac, the ETIAS Central System can use the ESP to compare the data in ETIAS with the data in Eurodac corresponding to individuals having left or having been removed from the territory of the Member States in compliance with a return decision or removal order.[400]

The 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 assessment's result is recorded only in the ETIAS application files.[401]

eee) *VIS*

As mentioned, Eurodac is connected to the ESP – not only to enable the automated processing with ETIAS but also with the VIS.[402] Relevant data in the VIS are compared to relevant data in Eurodac.[403]

Visa authorities may directly consult Eurodac in a read-only format for the purpose of manually verifying hits triggered by the automated

396 Interoperability Regulation - Judicial Cooperation, Art 6.
397 Eurodac Regulation 2024, Art 8(1); ETIAS Regulation, Art 11 and 20.
398 Eurodac Regulation 2024, Art 8(2); ETIAS Regulation, Art 20, 22 and 26.
399 ETIAS Regulation, Art 20(2)(a), (g), and (i).
400 Eurodac Regulation 2024, Art 8(2).
401 ibid, Art 9.
402 ibid, Art 11 in conjunction with Amendment to the VIS Regulation 2021, Art 9(a).
403 Eurodac Regulation 2024, Art 11.

queries carried out by the VIS[404] and examining/deciding on visa applications.[405,406]

fff) *Third Countries, Private Entities and International Organisations*

Personal data obtained by a Member State or Europol from Eurodac must not be transferred or made available to any third country, international organisation, or private entity established in or outside the Union. This prohibition also applies if those data are further processed at national level or between Member States.[407]

However, personal data which originated in a Member State and are exchanged between Member States or between a Member State and Europol, following a hit obtained for law enforcement purposes, can be transferred to third countries under certain circumstances. Transmission is permitted if there is no "real risk" that the data subject may be subjected to torture, inhuman or degrading treatment or punishment, or any other violation of their fundamental rights as a result of the transfer.[408] Regarding data exchanged with Europol, a data transfer is permitted only if it is necessary and proportionate to cases falling within Europol's mandate, and the Member State of origin provides consent.[409]

Furthermore, data can be shared with third countries for the purpose of return. This is, however, also conditional. Data transfers must be in accordance with the GDPR.[410] Also, data can be transferred or made available solely for the purpose of identifying and issuing an identification or travel document to an illegally staying third-country national for the purposes of return. The third-country national concerned must have been informed

404 In accordance with Amendment to the VIS Regulation 2021, Art 9(a) and 9(c).
405 In accordance with Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 Establishing a Community Code on Visas [2009] OJ L243/1 (Visa Code), Art 21.
406 Eurodac Regulation 2024, Art 10.
407 ibid, Art 49(1) in conjunction with GDPR Art 4(2); Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard 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, and on the Free Movement of Such Data [2016] OJ L119/89 (Police Directive), Art 2.
408 Eurodac Regulation 2024, Art 29(2), (3).
409 ibid, Art 49(3).
410 ibid, Art 50(2).

that their personal data may be shared with the authorities of a third country.[411] Data can also be shared according to the GDPR, e.g., when the transfer is necessary for important reasons of public interest.[412] Such transfers, based on the Eurodac Regulation or the GDPR, are subject to monitoring by the independent supervisory authority.[413] In any case, the transfers of personal data to third countries pursuant to this article shall not prejudice the data subject's right in the Eurodac Regulation, in particular with regard to non-refoulement.[414]

ggg) *eu-LISA*

eu-LISA is, as mentioned, responsible for the operational management of Eurodac.[415] The agency can access and use actual personal data from the Eurodac production system for testing purposes, including diagnostics and repairs when faults are identified, as well as for testing new technologies and techniques aimed at enhancing Eurodac's performance or the transmission of data to it.[416] Real personal data adopted for testing has to be rendered anonymous in such a way that the data subject is no longer identifiable.[417] As already mentioned, eu-LISA also accesses Eurodac data to draw up statistics.[418]

III. Interoperability

1. Connecting the European Union's Migration Information Systems

The Interoperability Regulations are the result of recommendations by an expert group convened by the European Commission in 2017. They suggested a European Search Portal to search across all relevant migration information systems simultaneously, a shared Biometric Matching Service

411 ibid, Art 50(3).
412 ibid, Art 50(4) in conjunction with GDPR, Art 49(1)(d).
413 Eurodac Regulation 2024, Art 50(4); GDPR, chap VI.
414 Eurodac Regulation 2024, Art 50(5).
415 ibid, Art 4(1).
416 ibid, Art 4(2)(a) and (b).
417 ibid, Art 4(2).
418 ibid, Art 12.

to process biometric data from all existing and new information systems, reducing costs and complexity, and a Common Identity Repository to allow a complete view of all claimed biographic identities used by a person.[419] Legal proposals from the European Commission followed in December 2017, adding a further element: a Multiple Identity Detector that would search across biometric and biographic data from all existing systems simultaneously.[420] On 20 May 2019, Regulation (EU) 2019/817, which establishes a framework for interoperability between EU information systems in the fields of borders and visas, and Regulation (EU) 2019/818, which establishes a framework for interoperability between EU information systems related to police and judicial cooperation, asylum, and migration, were adopted.[421]

The Interoperability Regulations provide the legal basis for the interconnection of six EU information systems: EES, SIS, VIS, ETIAS, ECRIS-TCN, and Eurodac. These six centralised databases now serve as building blocks: personal data are extracted from them and used to construct new systems, with the aim of making the data accessible to a wider number of authorities and using it in ways not initially foreseen in the legislation governing the underlying databases.[422] Although these new regulations seem already quite comprehensive, the Commission has announced that further centralisations are possible in the future: "Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the [interoperability] components".[423]

419 Costica Dumbrava, 'Interoperability of European Information Systems for Border Management and Security' (European Parliamentary Research Service 2017) Briefing PE 607.256.

420 Proposal for a Regulation on Establishing a Framework for Interoperability between EU Information Systems (Police and Judicial Cooperation, Asylum and Migration) [2017] COM(2017)794 (Proposal for an Interoperability Regulation 2017 - Judicial Cooperation); Katrien Luyten and Sofija Voronova, 'Interoperability between EU Border and Security Information Systems' (EPRS 2019) Briefing PE 628.267.

421 Interoperability Regulation - Borders; Interoperability Regulation - Judicial Cooperation.

422 Jones, 'Data Protection, Immigration Enforcement and Fundamental Rights' (n 28) 16.

423 Proposal for an Interoperability Regulation 2017 - Judicial Cooperation.

2. Legal Basis and Purpose: Regulation (EU) 2019/818

The legal basis for interoperability consists, as mentioned, of two Regulations: Regulation (EU) 2019/817 and Regulation (EU) 2019/818.[424] This was necessary because of differences in participation in the underlying information systems of some Member States and the Schengen/Dublin associated countries.[425] Regulation (EU) 2019/818 applies, according to its Art. 3, to Eurodac, SIS, ECRIS-TCN, and Europol. Regulation (EU) 2019/817 applies to the EES, VIS, ETIAS, and SIS.[426] The two regulations contain largely identical provisions. Accordingly, when this study refers to the Interoperability Regulation, it means Regulation (EU) 2019/818, unless it refers to differences that arise between the two regulations and explicitly mentions Regulation (EU) 2019/817.

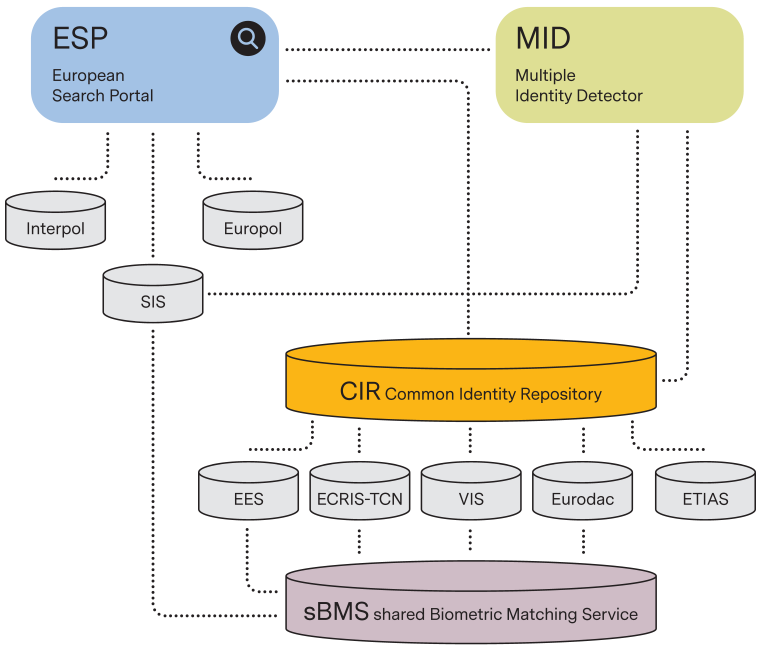
The objectives of the Interoperability Regulations are primarily related to security and migration. These include enhancing the effectiveness and efficiency of border checks at external borders, contributing to the prevention and combating of illegal immigration, supporting and improving visa policy and the examination of asylum applications, serving law enforcement purposes, and facilitating the identification of certain unknown persons. The Interoperability Regulations achieve these goals primarily with the introduction of technical tools, discussed in the next sections.

3. Components of the Interoperability System

eu-LISA is responsible for the development of the interoperability components and for any adaptations required for establishing interoperability between the central systems of the EES, VIS, ETIAS, SIS, Eurodac, ECRIS-TCN, and the European Search Portal (ESP), the shared Biometric Matching Service (sBMS), the Common Identity Repository (CIR), the Multiple Identity Detector (MID), and the Central Repository for Reporting and Statistics (CRRS).[427] The interoperability components are hosted

424 Interoperability Regulation - Borders; Interoperability Regulation - Judicial Cooperation.
425 ibid.
426 Interoperability Regulation - Borders, Art 3.
427 ibid, Art 54(3); Interoperability Regulation - Judicial Cooperation, Art 54(3).

by eu-LISA in its technical sites.[428] Following the entry into operations of each interoperability component, eu-LISA is responsible for the technical management of the central infrastructure of the interoperability components, including their maintenance and technological developments.[429] The agency also ensures that the central infrastructures of the interoperability components are operated in accordance with the Interoperability Regulations.[430]



428 Interoperability Regulation - Border, Art 54(2); Interoperability Regulation - Judicial Cooperation, Art 54(2).
429 ibid, Art 55(1).
430 ibid, Art 54(3).

a) *European Search Portal (ESP)*

The European Search Portal (ESP) was established for the purposes of "facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems, to Europol data and to the Interpol databases."[431] The ESP primarily consists of a central infrastructure, including a search portal enabling the simultaneous querying of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN, as well as of Europol data and the Interpol databases.[432] Furthermore, it entails a communication channel between the ESP, Member States, and Union agencies, as well as a communication infrastructure between the ESP and the information systems, including Europol data and Interpol databases and the central infrastructures of the CIR and the MID.[433]

The ESP is used by all the Member State authorities and Union agencies that have access to at least one of the underlying information systems, to the CIR, the MID, to Europol data, or one of the Interpol databases.[434] Each authority or agency shall only be able to use the ESP to the extent it is granted access to the databases and information systems by law.[435] For its use, there are profiles of each category of ESP users and purposes, which comprise certain information, like the field of data used, the databases and EU information systems that can be queried, specific data that can be queried, and categories of data that may be provided.[436] ESP users launch a query by submitting alphanumeric or biometric data to the ESP. Once a query has been launched, the ESP queries the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, Europol data, and the Interpol databases simultaneously with the data submitted and in accordance with the user profile.[437] The information exchange is provided in the universal message format (UFM)[438] and can be accessed through an "interface control document" that is based on the UFM.[439] The reply provided by the ESP provides the data held by the information systems and databases mentioned and

431 ibid, Art 6(1).
432 ibid, Art 6(2).
433 ibid, Art 6(2)(b), (c).
434 ibid, Art 7(1).
435 ibid, Art 7(2).
436 ibid, Art 8(1).
437 ibid, Art 9(1).
438 ibid, Art 38. Any new information exchange models and information system in the area of Justice and Home Affairs shall use the UFM.
439 ibid, Art 9(3).

indicates the information system or database to which the data belongs. It should not contain data to which the user has no access under the law.[440] A fall-back procedure is foreseen in the Regulations for whenever it is technically impossible to use the ESP.[441]

eu-LISA has to keep logs of all data processing operations in the ESP.[442] The Member States must keep logs of queries their authorities and their staff made into the ESP.[443] The logs can 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. Logs are erased after one year, unless they are required for monitoring procedures that have already begun. Then, they shall be erased once the monitoring procedures no longer require the logs.[444]

b) *shared Biometric Matching Service (sBMS)*

The sBMS was established in order to support the CIR, the MID, and the objectives of the EES, VIS, Eurodac, SIS, and ECRIS-TCN. The sBMS stores biometric templates obtained from the biometric data. These are stored in the CIR and SIS, which enables querying with biometric data across several EU information systems.[445]

The shared BMS consists of a central infrastructure that replaces the existing central systems of the EES, VIS, SIS, Eurodac, and ECRIS-TCN. This infrastructure stores biometric templates, facilitates searches using biometric data, and provides a secure communication framework between the shared BMS, Central SIS, and the CIR. For each set of data, the shared BMS includes, in each biometric template, a reference to the EU information systems in which the corresponding biometric data are stored, along with a reference to the actual records in those EU information systems.[446] The CIR and SIS use the biometric templates stored in the shared BMS each time they search biometric data stored within their own systems.[447]

440 ibid, Art 9(4).
441 ibid, Art 11.
442 ibid, Art 10(1).
443 ibid, Art 10(2).
444 ibid, Art 10(3).
445 ibid, Art 13(1).
446 ibid, Art 13(2).
447 ibid, Art 14.

The biometric data in question is stored in the sBMS for as long as the corresponding data are stored in the CIR or SIS.[448] eu-LISA keeps logs of all data processing operations in the shared BMS, while each Member State keeps logs of queries by its authorities and staff.[449] 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.[450]

c) *Common Identity Repository (CIR)*

The CIR was established for the purpose of "facilitating and assisting in the correct identification of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN, of supporting the functioning of the MID and of facilitating and streamlining access by designated authorities and Europol to the EES, VIS, ETIAS and Eurodac, where necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences".[451] The CIR creates an individual file for each person who is registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, containing certain data. These data include names, place and date of birth, as well as fingerprints.[452] For each set of data, the CIR incorporates a reference to the EU information systems to which the data belong.[453]

448 ibid, Art 15.
449 ibid, Art 16(1), (2).
450 ibid, Art 16(3).
451 ibid, Art 17(1).
452 Interoperability Regulation - Borders, Art 17(1) in conjunction with ECRIS-TCN Regulation. A full list of the data is here: surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, as well as, where available, information on travel documents. fingerprint data that have been collected in accordance with national law during criminal proceedings; as a minimum, fingerprint data collected on the basis of either of the following criteria: where the third-country national has received a custodial sentence of at least 6 months or where the third-country national has been convicted of a criminal offence which is punishable under the law of the Member State by a custodial sentence of a maximum period of at least 12 months (The fingerprint data shall have the technical specifications for the quality, resolution and processing of fingerprint data. The reference number of the fingerprint data of the convicted person shall include the code of the convicting Member State).
453 Interoperability Regulation - Borders, Art 18(2); Interoperability Regulation - Judicial Cooperation, Art 18(2).

The CIR is composed of a central infrastructure that replaces the central systems of, respectively, the EES, VIS, ETIAS, Eurodac, and ECRIS-TCN, to the extent that it stores the data in question. It also contains a secure communication channel between the CIR, Member States, and Union agencies that are entitled to use the CIR, a secure communication infrastructure between the CIR and the information systems, as well as one with the central infrastructures of the ESP, the shared BMS, and the MID.[454] Whenever data are added, amended, or deleted in one of the information systems, the data stored in the individual file of the CIR have to be updated accordingly.[455]

The CIR may be accessed for the identification of persons by police authorities, for the detection of multiple identities, or for the purpose of preventing, detecting, or investigating terrorist offences or other serious criminal offences.[456]

Police authorities can query the CIR in a wide range of circumstances: when they are unable to identify a person, should doubts arise regarding the identity data or the authenticity of the travel document provided by a person, whenever there are doubts as to the identity of the holder of a travel document, or whenever a person is unable or refuses to cooperate.[457] They can check data of children from the age of twelve years.[458] The CIR is queried with the biometric data of the person concerned, taken live during an identity check, during which the person has to be present.[459] Should the query indicate that data on that person are stored in the CIR, the police authority gains access to consult data on names, including aliases and previous names, date and place of birth, nationalities, as well as gender of the person stored in the CIR.[460] Whenever the biometric data of the person cannot be used or if the query fails, a search can be carried out with the person's identity data, in combination with travel document data, or with the identity data provided by that person.[461]

454 ibid, Art 17(2).
455 ibid, Art 19.
456 ibid, Art 20, 21 and 22.
457 ibid, Art 20(1) (a - e).
458 ibid, Art 20(1).
459 ibid, Art 20(2); ibid, Art 22(4) only in the event of a natural disaster, an accident or a terrorist attack and solely for the purpose of identifying unknown persons who are unable to identify themselves or unidentified human remains, the police authority can query the CIR with the biometric data of those persons.
460 ibid, Art 20(3) in conjunction with ibid, Art 18(1).
461 ibid, Art 20(3).

The second reason for accessing the CIR is for specific national authorities, i.e., to detect multiple identities. This occurs when a query of the CIR generates a yellow link created by the MID, which will be explained in the following section.[462] The authority "responsible for the manual verification of different identities"[463] has access to CIR data connected by the yellow link for the purpose of the verification of the person's identity. Whenever a query of the CIR results in a red link created by the MID, all Member State authorities and Union agencies with access to at least one EU information system included in the CIR or to SIS can access the data stored in the CIR associated with the red link for the purpose of combating identity fraud.[464]

Third, where there are "reasonable grounds to believe that consultation of EU information systems will contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences", the law enforcement authorities designated by the Member States and Europol can consult the CIR in order to obtain information on whether data on a specific person are present in Eurodac, EES, VIS, or ETIAS.[465] When the CIR indicates that data on an individual are present in Eurodac, EES, VIS, or ETIAS in response to a query, it provides designated authorities and Europol with a reference indicating which information system contains the matching data. This reply should only be used for the purposes of submitting a request for full access, in the correct procedure, and only if the relevant law allows for it.[466] In the case of Eurodac, the procedure and conditions stated in Art. 32 ff., as explained above, would have to be followed. If no request is initiated following a match indicating data in one of the information systems, Europol or the designated authority must record a justification for this decision.[467]

Data stored in the CIR must be deleted automatically, in accordance with the data retention provisions in the regulations of the information systems.[468] The individual file is stored in the CIR for as long as the corresponding data are stored in at least one of the EU information systems. This time period shall not be influenced by the fact that data are linked.[469]

462 ibid, Art 21(1).
463 In accordance with ibid, Art 29.
464 ibid, Art 21.
465 ibid, Art 22(1).
466 ibid, Art 22(2), (3).
467 ibid, Art 22(2).
468 ibid, Art 23(1).
469 ibid, Art 23(2).

eu-LISA has to keep logs of all data processing operations in the CIR, while each Member State keeps logs of queries by its authorities.[470] As with the ESP and the shared BMS, the logs may be used only for data protection monitoring.[471]

d) *Multiple-Identity Detector (MID)*

The multiple-identity detector is established for the purpose of supporting the functioning of the CIR and the objectives of the information systems.[472] The MID creates and stores so-called identity confirmation files. These contain links between data in the EU information systems included in the CIR and SIS. It is supposed to detect multiple identities, with the purpose of facilitating identity checks and combating identity fraud.[473] The identity confirmation files contain the following information: the links described below, a reference to the EU information systems wherein the linked data are held, a single identification number allowing retrieval of the linked data from the corresponding EU information systems, an indication of the authority responsible for the manual verification of different identities, and the date of creation of the link or of any update to it.[474]

The MID is composed of a central infrastructure; it stores links and references to EU information systems and a secure communication infrastructure, meant to connect the MID with the SIS and the central infrastructures of the ESP and the CIR.[475]

A multi-identity detection is initiated whenever a file is created or updated in the EES, VIS, or ETIAS, when a dataset is transmitted to Eurodac, or when data are created or modified in the ECRIS-TCN. It also occurs when an alert regarding a person is created or updated in the SIS.[476] If biometric data are stored in the information system, the shared BMS is used in order to perform the multiple-identity detection. It will compare the biometric templates obtained from any new biometric data to the biometric templates

470 ibid, Art 24.
471 ibid, Art 24(4).
472 ibid, Art 25(1).
473 ibid, Art 25(1).
474 ibid, Art 34.
475 ibid, Art 25(2).
476 ibid, Art 27(1).

already contained in the shared BMS.[477] The CIR and the SIS are utilised to do the same with biographic and travel document data.[478]

Should no match be reported upon a multi-identity detection being launched, the normal process of creating or updating a file, data set, or an alert continues. If, however, a query reports one or several matches, the CIR and, where relevant, SIS create a link between the data used to launch the query and the data triggering the match.[479] A white link is attached to the file, whenever the linked files are the same or similar. This means that they belong to the same person and contain the same data. Thus, no manual processing is necessary.[480] A yellow link is attached to the file, if the linked files cannot be considered to be similar; a manual verification of the matching sets of data is required in order to determine how the matching data should be classified: as green, red, or white.[481] The links are stored in the identity confirmation file.[482] Once the yellow link between data is created, the competent authority immediately has to access the MID in order to verify the different identities manually.[483] The authority responsible for the verification process depends on the place of storage of data. In the case of Eurodac, authorities competent to collect the data in the CIR data set are responsible.[484] Once these authorities have verified the identities, they attach the matching link to the file:

Green Link

The authorities add a green link when the manual verification reveals that identical (or very similar) biographic identities have been detected; they have different biometric data. One may then conclude that the linked data refer to two different persons.[485]

477 ibid, Art 27(2).
478 ibid, Art 27(3).
479 ibid, Art 28(2).
480 ibid, Art 28(3).
481 ibid, Art 28(4).
482 ibid, Art 28(6).
483 ibid, Art 29.
484 Interoperability Regulation - Judicial Cooperation, Art 29(1) (c-h).
485 Interoperability Regulation - Borders, Art 31; Interoperability Regulation - Judicial Cooperation, Art 31.

Red Link

A red link is created when multiple files contain the same biometric data but different biographic data, and an official concludes that this is the result of identity fraud.[486]

White Link

A white link is created when the same person exists in multiple systems (the same biometric data and the same, or very similar, biographic data in different files), or an investigation indicates that files hold the same biometric data but lawfully differing biographic data (for example, individuals who have changed their name or use an artistic persona).[487]

The application of green, red, or white links to matching data sets also gives rise to differing levels of access, for a variety of authorities, to identity data stored in the CIR and SIS and the related data stored in the MID.[488]

In the case of a red link – a presumption of identity fraud – the rules appear to be contradictory. The Interoperability Regulations state that any national authority or EU agency that has access to at least one EU information system included in the CIR, or to the SIS, shall have access to two of the components of the identity confirmation file in question: the red link itself and the reference to the EU information systems wherein the linked data are held.[489] Conversely, the regulations also state that: "Where the CIR or SIS are queried and where a red link exists between data in two or more of the EU information systems, the MID shall indicate the data [contained in the identity confirmation file]"[490] – that is, all the data contained in the file, rather than just two components.

In the case of a white link, access to the linked data will be granted to national authorities or EU agencies that have access to both EU information

486 ibid, Art 32.
487 ibid, Art 33.
488 Jones, 'Data Protection, Immigration Enforcement and Fundamental Rights' (n 28) 28.
489 Interoperability Regulation - Borders, Art 26(2) in conjunction with ibid, 34(a) and (b); Interoperability Regulation - Judicial Cooperation, Art 26(2) in conjunction with ibid, 34(a) and (b); Jones, 'Data Protection, Immigration Enforcement and Fundamental Rights' (n 28) 28ff.
490 Interoperability Regulation - Borders, Art 32(2) in conjunction with ibid, Art 34; Interoperability Regulation - Judicial Cooperation, Art 32(2) in conjunction with ibid, Art 34; Jones, 'Data Protection, Immigration Enforcement and Fundamental Rights' (n 28) 29.

systems involved in the creation of the white link.[491] In the case of a query to the CIR or SIS indicating the existence of a white link, the MID will confirm that the identity data of the linked records correspond to the same individual.[492] The queried EU information systems will also indicate all the linked data on the person, if the authority launching the query has access to the linked data under Union or national law.[493] For example, if a visa applicant previously has applied for international protection, this might be visible to the visa authority.

National authorities or EU agencies will be granted access to green links if they have access to both EU information systems containing the data between which the green link was created, and a query of those information systems has confirmed a match between the two linked data sets.[494] Following queries of the CIR or the SIS that indicate the existence of a green link, the MID shall indicate that the identity data of the linked data do not correspond to the same person.[495]

The identity confirmation files and the data in them, including the links, are stored in the MID for as long as the linked data are stored in two or more EU information systems.[496] eu-LISA keeps logs of all data processing operations in the MID. Each Member State and Union agency keeps logs of queries that its authorities and/or staff respectively make to use the MID.[497]

4. Common Provisions

There are common technical tools supporting interoperability, which are explained in this chapter. In addition, the Interoperability Regulations contain common provisions on data protection, accountability, and access to remedies. The latter will be scrutinised more thoroughly throughout this study and not be discussed here.

491 Interoperability Regulation - Borders, Art 26(3); Interoperability Regulation - Judicial Cooperation, Art 26(3).
492 ibid, Art 33(2).
493 ibid, Art 33(2).
494 ibid, Art 26(4).
495 ibid, Art 31(2).
496 ibid, Art 35.
497 ibid, Art 36.

a) *The Web Portal*

A web portal is established for the purpose of facilitating the exercise of the right of access to, rectification, erasure, or restriction of personal data processing, albeit, so it seems, only with regard to the MID.[498] The web portal contains information on the rights to information and access, rectification, and erasure of personal data. It further entails a user interface, enabling persons whose data are processed in the MID and who have been informed of the presence of a red link to receive the contact information of the competent authority of the Member State responsible for the manual verification of different identities.[499] The web portal will also include a template e-mail to facilitate communication between the portal user and the authority responsible for the manual verification of different identities.[500]

b) *The Central Repository for Reporting and Statistics (CRRS)*

A CRRS is established that is supposed to support the objectives of the information systems and "provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes."[501] eu-LISA establishes, implements, and hosts the CRRS in its technical sites. The data contained in CRRS will not allow for the identification of individuals.[502] Access to the CRRS is granted to various bodies and agencies in the Union.[503]

498 ibid, Art 49(1).
499 ibid, Art 49(2).
500 ibid, Art 49(3).
501 ibid, Art 39(1).
502 ibid, Art 39(3).
503 ibid, Art 39(2) refers to authorities referred to in Regulation (EU) 2018/1862 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 Police Cooperation and Judicial Cooperation in Criminal Matters [2018] OJ L312/56 (SIS III - Police Regulation), Art 74, and of ECRIS-TCN Regulation, Art 32; eu-LISA shall provide the European Parliament, the Council, the Member States, the Commission, Europol, Eurojust, the European Border and Coast Guard Agency and the European Data Protection Supervisor with any statistical reports that it produces (SIS III - Police Regulation, Art 74(6)); The duly authorised staff of eu-LISA, of the competent authorities and of the Commission shall have access to the data processed within ECRIS-TCN solely for the purposes of reporting and providing

The Interoperability Regulations stipulate that, for reporting and statistical purposes, competent authorities of the Member States, the Commission, and eu-LISA have access to consult specific data related to ESP, the CIR, and MID. This includes information such as the number of queries, types of links, nationality, gender, year of birth of individuals, and the type of travel document used.[504] The EBCG Agency has access to the same data for carrying out "risk analyses and vulnerability assessments".[505] Europol has access only to the data in the CIR and MID for the purpose of carrying out "strategic, thematic and operational analyses".[506] Upon request, relevant information has to be made available by the Commission to the European Union Agency for Fundamental Rights in order to evaluate the impact of the Interoperability Regulations on fundamental rights.[507]

c) *Security, Data Controllers and Processors*

eu-LISA, the ETIAS Central Unit, Europol, and the Member State authorities have to ensure the security of the processing of personal data that takes place pursuant to the Interoperability Regulations.[508] The Member State authorities that act as controllers for the respective information systems are also the controllers of the biometric templates stored by the BMS, the CIR,[509] and the MID.[510] Regarding the latter, if information is processed by the ETIAS Central Unit and the EBCG Agency, these entities are considered the data controllers.[511] In relation to the processing of personal

statistics, without allowing for individual identification (ECRIS-TCN Regulation, Art 32(1)).

504 Interoperability Regulation - Borders, Art 66(1-3); Interoperability Regulation - Judicial Cooperation, Art 62.

505 Interoperability Regulation - Borders, Art 66(4); Interoperability Regulation - Judicial Cooperation, Art 62(4).

506 Interoperability Regulation - Borders, Art 66(5); Interoperability Regulation - Judicial Cooperation, Art 62(4).

507 Interoperability Regulation - Borders, Art 66(7); Interoperability Regulation - Judicial Cooperation, Art 62(7).

508 ibid, Art 42.

509 ibid, Art 40(1), (2).

510 ibid, Art 40(3)(b).

511 ibid, Art 40(3)(a).

data in the shared BMS, the CIR, and the MID, eu-LISA acts as the data processor.[512]

512 ibid, Art 41.