VIII. Making Data Available to Public-Sector Bodies based on Exceptional Need (Art. 14-22)

Chapter V ('Making Data Available to Public Sector Bodies, the Commission, the European Central Bank or Union Bodies based on Exceptional Need', Art. 14-22) creates a framework under which public-sector bodies may request certain data in specific scenarios, especially in the case of public emergencies, such as public health emergencies or major natural or human-induced disasters.[578] These provisions are meant to combat the lack of available data for the use in favour of the public good.[579]

These provisions seem especially relevant and timely after the global pandemic in general and the recent flood disasters in Germany, Austria and Slovenia in particular.[580] The provisions are seen as a "fundamental advancement in the recognition of the public utility of data, and sets proportionate – yet narrow – conditions under which this public utility takes precedence over private interests".[581]

1. Obligation to Make Data Available to Public-Sector Bodies (Art. 14)

Art. 14(1) obliges data holders, upon a duly reasoned request, to make data available to certain eligible bodies, where they demonstrate an exceptional need to carry out its statutory duties in the public interest. Only data holders that are a legal person other than public sector bodies are addressed. However, rec. 63 adds that the notion of data holder may include public undertakings. Eligible bodies include public sector bodies, the Commission, the European Central Bank or a Union body.

578 Commission, COM(2022) 68 final Explanatory Memorandum, p. 15.
579 Höne, M. / Knapp, J., *ZGI* 2023, 168.
580 Schaller, T. / Zurawski, P., *ZD-Aktuell* 2022, 01169.
581 Margoni, T. / Ducuing, C. / Schirru, L., Data property, data governance and Common European Data Spaces, May 2023, v. 0.4, p. 10.

Union and Public Sector Body

Union bodies means Union bodies, offices and agencies set up by or pursuant to acts adopted on the basis of the Treaty on European Union, the TFEU or the Treaty establishing the European Atomic Energy Community, Art. 2(27).

According to Art. 2(28) public sector body refers to national, regional or local authorities of the member states and bodies governed by public law of the member states, or associations formed by one or more such authorities or one or more such bodies. The term "public sector body" is exclusively relevant for Chapter V (Art. 14-22). According to rec. 63 research-performing organisations and research-funding organisations could also be organised as public sector bodies or as bodies governed by public law, thus being entitled to requests according to Art. 14.

It should be noted that this definition of public sector body differs from the definition in Art. 2(17) DGA, where instead of "national authorities" it reads "State". A broader understanding can be explained by the fact that while the DGA obliges the public sector body concerning the reuse of its data, under Chapter V of the Data Act data holders are obliged to make data available to them.

Material Scope of the Obligation to Make Data Available

The provisions establish the right for the public sector bodies to both access and use the data requested.[582] The request also encompasses the metadata necessary to interpret and use those data. In contrast to the user's right to data access in Art. 4(1), which is limited to data generated by the use of a product or related service, the obligations to make data available refer to all types of data.[583]

Rec. 63 further states public emergencies as primary examples for such an exceptional need. It adds that exceptional needs are circumstances which are unforeseeable and limited in time, in contrast to other circumstances which might be planned, scheduled, periodic or frequent. The prerequisites for such an obligation are further defined in the following Art. 15-22.

582 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 109.

583 Regarding the access to and use of personal data it is still debated whether Art. 14 et seqq. fulfil the requirements for a legal basis according to Art. 6(1)(c) and (e) GDPR. (see below VIII.11.).

Rec. 64 justifies the obligation based on the assessment that in such cases of public emergency the public interest "will outweigh the interests of the data holders to dispose freely of the data they hold". However, the interests of data subjects whose personal data is made available are not addressed. Some argue that the rights under Art. 15, 16 and 17 CFREU of the data subjects might be affected.[584]

If data holders do not comply with this obligation, they may face sanctions according to Art. 40.[585]

In the original proposal small and micro enterprises as defined in Art. 2 of the Annex to Recommendation 2003/361/EC were exempted from the obligation to make data available, Art. 14(2). As proposed by the MPIIC Statement, the JURI Draft opinion and the Council Presidency in its compromise text, this exemption was deleted.[586] This change is in line with the aim of this chapter, as public emergencies require broadest possible access to data and in these cases the public interest outweighs the interests of the data holders to dispose freely of the data they hold (rec. 63) as well as the expected burden on small and micro enterprises. However, SMEs are only obliged to provide data in situations of exceptional need to respond to a public emergency, rec. 63 (cf. Art. 15 (a)).

Considering the importance of access to relevant data, it is questionable whether access in cases of public emergencies is sufficient to further the fulfilment of tasks in the public interest.[587] Especially concerning non-personal data, lesser requirements for access rights of public sector bodies are conceivable and should have been considered. However, instead of expanding access rights concerning non-personal data, the scope of Art. 14 was narrowed by limiting scenarios under Art. 15(b) (former Art. 15(b) and (c)) to concern only the making-available of non-personal data. In general, the requirements for the different scenarios of exceptional need are stricter compared to the draft version. Respective amendments reduced the material scope of the obligation drastically.

584 Höne, M. / Knapp, J., *ZGI* 2023, 168, 169.
585 Klink-Straub, J. / Straub, T., *ZD-Aktuell* 2022, 01076.
586 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 49 n. 133, JURI PE736.696, pp. 12, 40, https://www.euractiv.com/section/data-privacy/news/swedish-presidency-tries-to-close-in-on-the-data-act/.
587 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (826).

2. Definition of Exceptional Need (Art. 15)

The reference point for the obligation to make data available are the circumstances under which public sector bodies may request data from private data holders. Art. 15(1) defines two scenarios which may constitute an exceptional need, which should be limited in time and scope.

Response to a Public Emergency

According to Art. 15(1)(a), an exceptional need is given where the data requested is necessary to respond to a public emergency and the public sector body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions. This means that the request under Art. 14 does not have to be the last resort.[588]

Definition of Public Emergency

According to Art. 2(29) public emergency means an exceptional situation, limited in time which is negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State(s). Art. 2(29) gives public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, including major cybersecurity incidents as examples for a public emergency.

Like "public sector body", the term "public emergency" is exclusively relevant for Chapter V and is only used in Art. 15, 18, and 20.

It is highly questionable whether providing the examples for public emergencies in the definition additionally to rec. 63 is helpful. It inflates the definition without adding to its understanding, as the examples were already provided in the recital.

Whether such a public emergency exists shall be determined or officially declared "according to the relevant procedures under Union or national law", Art 2(29). This may lead to various different procedures in the member states to determine a public emergency in the individual member states.

588 Schröder, M., *MMR-Beil.* 2024, 104 (105); Höne, M. / Knapp, J., *ZGI* 2023, 168 (169).

Instead, a standard European procedure could lead to more legal certainty regarding the obligation to make data available in cases of exceptional need.

Fulfilling a Specific Task in the Public Interest

An exceptional need may also exist according to Art. 15(1)(b) where the eligible body has identified specific data, the lack of which prevents it from fulfilling a specific task in the public interest, that has been explicitly provided by law, Art. 15 (1)(b)(i). Art. 15(1)(b) further gives official statistics or the mitigation or recovery from a public emergency as examples. In these non-emergency situations only non-personal data can be requested.

Rec. 65 adds that the eligible body should have "identified specific data that could not otherwise be obtained in a timely and effective manner and under equivalent conditions". This further requires that it has exhausted all other means at its disposal to obtain such data, including, but not limited to, purchase of the data on the market by offering market rates or relying on existing obligations to make data available, or the adoption of new legislative measures which could guarantee the timely availability of the data, Art. 15(1)(b)(ii). This requirement might "incentivise data holders to make data available beforehand and systematically".[589] Nevertheless, it remains unclear which efforts the eligible bodies should make before requesting the data.[590]

According to Art. 15(3), the obligation to demonstrate that the public sector body was unable to obtain non-personal data by purchasing them on the market shall not apply where the specific task carried out in the public interest is the production of official statistics and where the purchase of such data is not allowed by national law.

Art. 15(1)(b) does not apply to SMEs, Art. 15(2).

Assessment of the Definitions

While the definition in Art. 2(29) and the scenario of Art. 15(1)(a) seem to give a narrow and strict understanding of an exceptional need, this

589 Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 63.

590 Cf. Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 63.

understanding is expanded in Art. 15(b) regarding time as well as intensity.[591] Although this is reflected in the increasing requirements for the data request, some had argued to concretise the conditions for an exceptional need.[592] According to the BDI, the definitions of "public emergency" and also "fulfilling a specific task in the public interest that has been explicitly provided by law" are too broad and lack legal certainty for the data holders, when the obligation to make data available exists.[593]

Regarding the necessary differentiation between Art. 15(1)(a) and (b) in some scenarios of public emergency, for example a pandemic, it might be difficult to effectively distinguish between response, prevention, and recovery.[594] However, this differentiation remains necessary, due to different requirements in paras. (a) and (b) and its link to the possibility to claim compensation, Art. 20. Respective difficulties in the application of Art. 15 could have been minimised by combining the response to a public emergency with the prevention of and recovery from it together in Art. 15(1)(a) as proposed by the JURI Draft Opinion.[595]

Concerning the prerequisites of Art. 15(1)(b)(ii) it remains open, whether "purchasing the data on the market" refers only to data already offered on the market or if the public sector body is also required to individually negotiate with potential data providers, if the needed data has not been offered.[596] It is argued that it should be understood as data that is "actually offered to the public".[597] Furthermore, it should be clarified how to determine the "market rate", as single-source data would be prone to monopoly pricing.[598]

It seems questionable, how the requirement that the exceptional need should be limited in time and scope is consistent with the possibility of existing obligations to make data available or the adoption of new legislative

591 Cf. also Schaller, T. / Zurawski, P., *ZD-Aktuell* 2022, 01169.
592 Cf. also Schaller, T. / Zurawski, P., *ZD-Aktuell* 2022, 01169; Hilgendorf, E. / Vogel, P., *JZ* 2022, 380 (388).
593 BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 18.
594 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 48.
595 JURI PE736.696, p. 40.
596 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 50, 51 n. 137.
597 Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 63.
598 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 51 n. 137; Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 63.

measures which could guarantee the timely availability of the data, to which Art. 15(1)(b)(ii) refers.

The requirement that the data could not be obtained by measures such as the purchase on the market or the adoption of new legislative measures limits the scope of application of this case of exceptional need drastically.[599]

3. Relationship with Other Obligations to Make Data Available (Art. 16)

Existing Obligations to Make Data Available

According to Art. 16(1) the provisions of Chapter V should not affect existing obligations in Union or national law of reporting and complying with information requests. Rec. 66 explains further that "obligations placed on data holders to provide data that are motivated by needs of a non-exceptional nature, notably where the range of data and of data holders is known and where data use can take place on a regular basis, as in the case of reporting obligations and internal market obligations, should not be affected". The same applies to existing obligations to demonstrate or verify compliance with legal obligations. According to rec. 66 this includes "cases where public sector bodies assign the task of the verification of compliance to entities other than public sector bodies".

These provisions together show that Chapter V only regulates "ad hoc" data access and thus should only pre-empt national legislation concerning ad hoc data access.[600] This is also evident in the first sentence of Art. 15(1).

In addition to Art. 1(6) sent. 1 and Art. 16(1), rec. 66 clarifies that this regulation neither applies to nor pre-empts "voluntary arrangements for exchange of data between private and public entities". The provisions do not address the possibility that such voluntary agreements could explicitly rule out the application of the rules under Chapter V.[601]

Art. 16(1) is expanded by rec. 67 which reads that the Data Act complements and is without prejudice to the Union and national laws providing for the access to and enabling to use data for statistical purposes, in partic-

599 Schröder, M., *MMR-Beil.* 2024, 104 (105); similarly also Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (824).

600 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 53 n. 145.

601 Cf. Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 67.

ular Regulation (EC) No 223/2009 on European statistics and its related legal acts as well as national legal acts related to official statistics.

The Prevention, Investigation and Prosecution of Criminal and Administrative Offences

Art. 16(2) excludes the prevention, investigation, detection or prosecution of criminal or administrative offences, or the execution of criminal penalties, as well as customs or taxation administration as possible scenarios in which an exceptional need may occur. Therefore, concerning these areas "public sector bodies should rely on their powers under sectoral legislation" (rec. 60).

Correspondingly, the Union and national law applicable in these areas is not affected by Chapter V, as is also stated by Art. 1(4) for the entire Data Act. Art. 16(2), however, adds that applicable law on the prosecution of administrative offences and execution of administrative penalties should not be affected.

Art. 16(2) and Art. 19(1) together ensure the data made available is only used for the intended purposes.[602]

4. Requirements for the Request to Make Data Available (Art. 17 paras. 1 and 2)

Rec. 69 states the necessity for a "proportionate, limited and predictable framework at Union level […] to ensure legal certainty and to minimise the administrative burdens placed on businesses". Hence, Art. 17 lays down requirements for requests for data to be made available in cases of exceptional need. These provisions ensure that the public sector body has to prove in its request the exceptional need and the conditions of the obligation to make data available.[603] It gives the data holder precise information about the request and thus reduces the data holder's burden.[604] However, the public sector body may face difficulties specifying the data required, as it may

602 Klink-Straub, J. / Straub, T., *ZD-Aktuell* 2022, 01076.
603 Schaller, T. / Zurawski, P., *ZD-Aktuell* 2022, 01169.
604 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 110.

often not know which data private entities hold.[605] As the data holder can decline a request due to unavailability of the data, information imbalances could reduce the effectiveness of this data access right.[606]

Information To Be Provided

The precise information to be given in the context of a request pursuant to Art. 14(1) are according to Art. 17(1):

- specify what data are required, including metadata that is necessary to interpret and use that data (lit. a)
- demonstrate that the conditions necessary for the existence of the exceptional need as referred to in Article 15 for the purpose of which the data are requested are met (lit. b)
- explain the purpose of the request, the intended use of the data requested, including when applicable by a third party in accordance with paragraph 4, the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need (lit. c)
- specify, if possible, when the data is expected to be deleted by all parties that have access to it (lit. d)
- justify the choice of data holder to which the request is addressed (lit. e)
- specify any other public sector bodies, Union institutions, agencies or bodies and the third parties with which the data requested is expected to be shared with (lit. f)
- where personal data are requested, specify any measures necessary and proportionate to implement data protection principles, data protection safeguards such as the level of aggregation or pseudonymisation, and whether anonymisation can be applied by the data holder before making data available (lit. g)
- state the legal provision allocating to the requesting public sector body or to the Commission, the European Central Bank or Union bodies the specific public interest task relevant for requesting the data (lit. h)
- specify the deadline referred to in Art. 18 and by which the data are to be made available and within which the data holder may request the public

605 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 54 n. 148.

606 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 54 n. 148; Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 68.

sector body, the Commission, the European Central Bank or Union body to modify or withdraw the request (lit. i)
– make its best effort to avoid that compliance with the data request results in the data holders' liability for infringement of Union or national law (lit. j)

The provision of Art. 17(1)(j) implies a precedence of the obligation under Art. 14 DA over other legal obligations of the data holder, even if compliance leads to a liability of the data holder.[607]

Further requirements

Beyond these informational duties Art. 17(2) stipulates further requirements for the request. According to Art. 17(2)(a), the request must be made in writing and be expressed in clear, concise, and plain language understandable to the data holder. It must be specific with regards to the type of data requested and correspond to data which the data holder has control over at the time of the request, Art. 17 (2)(b).

According to Art. 17(2)(c), the request must be justified and proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested.

According to Art. 17(2)(d), the request must respect the legitimate aims of the data holder, committing to ensuring the protection of trade secrets in accordance with Article 19(3), and the cost and effort required to make the data available. For example, the deadline referred to in Art. 17(1)(i) must also consider legitimate aims and especially the time and effort needed to protect affected personal data as well as the time needed for its anonymisation and pseudonymisation, as required by Art.18(4).[608]

As the requirement of Art. 17(2)(d) demands subsequently for strong technical and legal safeguards to ensure the effective protection of trade secrets, the Centre for IT & IP Law (CiTiP) of the KU Leuven recommended that the Data Act should have required for public sector bodies to be equipped with the necessary legal, technical, and human resources to comply with these obligations.[609]

Rec. 69 adds that the burden on data holders should be minimised by obliging requesting entities to respect the once-only principle, which

607 Cf. Schröder, M., *MMR-Beil.* 2024, 104 (106).
608 BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 19.
609 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 49.

prevents the same data from being requested more than once by more than one public sector body where those data are needed to respond to a public emergency.

According to *Leistner and Antoine*, Art. 17(2)(c) and (d) ensure that the legitimate interests of the data holder are observed and – consequentially – achieve balanced and proportionate results.[610]

According to Art. 17(2)(e), the request must concern non-personal data, and only if this is demonstrated to be insufficient to respond to the exceptional need to use data, in accordance with Article 15(1)(a), request personal data in aggregated or pseudonymised form and set out the technical and organisational measures that will be taken to protect the data (rec. 72).

According to Art. 17(2)(f), the request must inform the data holder of the penalties that shall be imposed pursuant to Art. 40 by the competent authority referred to in Art. 37 in the event of non-compliance with the request.

According to Art. 17(2)(g) and to ensure transparency (rec. 69), the request should be transmitted to the data coordinator referred to in Art. 37 where the requesting public sector body is established, who shall make the request publicly available online without undue delay unless it considers that this would create a risk for public security. The Commission, the European Central Bank and Union bodies shall make their requests available online without undue delay and inform the Commission thereof.

In case personal data are requested, the request should be notified without undue delay to the independent supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the member state where the data holder is established, Art. 17(2)(i).

According to Art. 17(6) the Commission should develop a model template for requests pursuant to Chapter V. However, it is questionable whether a model template is suitable for the scenarios of exceptional need given in Art. 15, especially those according to lit. a.

5. Reuse of the Data Made Available (Art. 17 (3) and (4))

As the data obtained may be commercially sensitive, it should not be made available for reuse within the meaning of Directive (EU) 2019/1024 (Open

610 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 110.

Data Directive)[611] or the Data Governance Act. Correspondingly, the Open Data Directive and the Data Governance Act shall not apply to the data held by public sector bodies obtained pursuant to Chapter V, Art. 17(3). As not all obtained data will be commercially sensitive, it is questionable why the prohibition should apply to all data, especially since commercially sensitive data would be excluded from the scope of application of the Open Data Directive.[612] According to rec. 65, the data holder can expressly agree for the data to be used for other than the requested purposes. A similar approach, with the application of the Open Data Directive as the default and the possibility of the data holder to deny the re-use or to specify the purposes of the re-use, would have been more favourable.[613]

Nevertheless, as stated in rec. 70, the Open Data Directive is still applicable to the reuse of "official statistics for the production of which data obtained pursuant to this Regulation [the Data Act] was used, provided the reuse does not include the underlying data."

Furthermore, it must be noted that rec. 70 points to the option for public bodies to "[share] the data for conducting research or for the compilation of official statistics, provided the conditions laid down in this Regulation [the Data Act] are met". This is further regulated in Art. 21.

As the Open Data Directive only regulates the re-use of data, but does not provide access to data, access to data is still governed by national rules or sectoral EU or national legislation.[614] Thus, the Data Act does not exclude access of third parties to data obtained under Chapter V under existing legislation.[615] Although Art. 19(2)(b) limits the purposes for which data may be shared, it also indicates that the sharing of data received is not generally excluded.

However, according to Art. 17(4), Art. 17(3) does not preclude the public sector body to exchange the data obtained pursuant to Chapter V with other public sector bodies, in view of completing the tasks in Art. 15, as specified in the request in accordance with Art. 17(1)(f). It may also make

611 Directive (EU) 2019/1024 of the European Parliament and of the Council on open data and the re-use of public sector information.

612 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 56 n. 153.

613 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 56 n. 153.

614 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 57 n. 154.

615 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 57 n. 154.

the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. It is required to observe Art. 19.

The possibility to exchange data between public sector bodies given in Art. 17(4) is made necessary by the once-only principle according to rec. 69. However, it may lead to a circumvention of the requirements for a request according to Art. 17(1) and may dilute the consideration of the purpose for which the data were requested.[616]

Where a public sector body or a Union institution, agency, or body transmits or makes data available under Art. 17(4), it shall notify the data holder from whom the data was received without undue delay.

Where the data holder considers that its rights under Chapter V have been infringed by the transmission or making available of data, it may lodge a complaint with the competent authority designated pursuant to Art. 37 of the member state where the data holder is established, Art. 17(5).

6. Compliance with Requests for Data (Art. 18)

The data holder should comply with the request without undue delay, taking into account necessary technical, organisational and legal measures (Art. 18(1)). 'Complying' means making the data available, which has been sometimes understood as *in situ*-access to the data.[617] Against this interpretation, and in favor of a transfer of the data to the requesting body, speaks the obligation to erase the data, Art. 19(1)(c), as well as the possibility to share it with other public sector bodies, Art. 17(4), and research organisations, Art. 20, which requires prior transfer of the data to the requesting body. *Specht-Riemenschneider* also argues that such an *in situ*-access would not suffice for the purposes of Chapter V.[618]

The data holder may however decline the request or seek its modification under specific circumstances; for example if the data holder does not have control over the data requested (Art. 18(2)(a)) or if the request does not meet the conditions laid down in Art. 17(1) and (2) (Art. 18(2)(c)).

According to Art. 18(2)(b), the data holder may also decline or seek modification of the request if the data holder already provided the reques-

616 Schaller, T. / Zurawski, P., *ZD-Aktuell* 2022, 01169.
617 Schröder, M., *MMR-Beil.* 2024, 104 (106).
618 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (826).

ted data in response to previously submitted request for the same purpose by another public sector body or Union institution agency or body (*once only-principle*) and the data holder has not been notified of the destruction of the data pursuant to Art. 19(1)(c). While this principle is useful to minimise the burden on data holders and may incentivise a better cross-border coordination between public sector bodies, it may come into conflict with the public interest to respond to a public emergency timely and effectively.[619] As the MPIIC has pointed out, there may be cases where the public sector body which originally requested the data is no longer in the possession of the data or where it cannot provide the data in a timely manner to the public sector body in an exceptional need.[620] In these cases, if there is a public emergency according to Art. 15(a) the public interest should prevail over the interest to minimise the burden for data holders.[621]

According to Art. 18(3), a data holder – in the case of Art. 18(2)(b) – shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.

Decline or Seek for Modification

According to Art. 18(2) the decline or the seeking of modification must be made without undue delay and not later than within 5 working days in the case of a request for the data necessary to respond to a public emergency (Art. 15(1)(a)). In other cases of exceptional need the data holder should decline or seek modification without undue delay and not later than within 30 working days, Art. 18(2). Furthermore, rec. 71 states that the "data holder (…) should communicate the underlying justification for refusing the request to the" public sector body requesting the data. This requirement seems to only stem from the recitals.

Potential conflicts between the obligation to make data available and the *sui generis* database rights under the Directive 96/6/EC are not expressly addressed in the provisions, e.g., in Art. 18 or Art. 43. In addition, Art. 43 concerns only data obtained from or generated by a connected product or

619 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 55 n. 149.

620 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 55 n. 149.

621 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 55 n. 149.

related service. Regarding the access right under Art. 14 this leads to the questionable result that the applicability of the *sui generis* database rights depends on the way the data was generated. Only rec. 71 states that "where the *sui generis* database rights [...] apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body [...] from obtaining the data, or from sharing it, in accordance with" the Data Act. The phrasing of the recital corresponds to the provisions regarding the *sui generis* database rights in the Open Data Directive and the Data Governance Act.[622]

Art. 18(5) also states the possibility for the public sector body to challenge the data holder's refusal and the possibility for the data holder to challenge the request, if the matter cannot be solved by an appropriate modification of the request. The competent authority flows from Art. 37. However, the legal nature of this challenge, its procedure and its legal effects are not further specified in the Art. 37-42, though when the data holder refuses a request in cases of public emergencies a timely decision is urgent.[623]

Anonymisation and Pseudonymisation of Personal Data

If the requested dataset includes personal data the data holder shall anonymise it. Where the compliance with the request requires the disclosure of personal data, the data holder should aggregate or pseudonymise the data, Art. 18(4). According to rec. 64 the public sector body should demonstrate the strict necessity to use personal data and the specific and limited purposes for processing. Rec. 72 underlines that the "making available of the data and their subsequent use should be accompanied by safeguards for the rights and interests of individuals concerned by those data". If this provision was understood as regarding all individuals concerned in any way it would be hard to fulfil. A more practical interpretation would be to understand it as referring to data subjects within the meaning of the GDPR.

In cases of exceptional need not related to a public emergency, personal data cannot be requested, Art. 15(1)(b).

622 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 110; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 59 n. 161.

623 Cf. Schröder, M., *MMR-Beil.* 2024, 104 (106); corresponding changes were suggested by the Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 55 n. 150; Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 69.

7. Obligations of Public Sector Bodies Receiving Data (Art. 19)

Art. 19(1) obliges the public sector body receiving data pursuant to Chapter V to:

- not use the data in a manner incompatible with the purpose for which they were requested (lit. a);
- have implemented technical and organisational measures that preserve the confidentiality and integrity of the requested data and the security of the data transfers, in particular personal data, and safeguard the rights and freedoms of data subjects (lit. b);
- erase the data as soon as they are no longer necessary for the stated purpose and inform the data holder and individuals or organisations that received the data pursuant to Article 21(1) without undue delay that the data have been erased, unless archiving of the data is required in accordance with Union or national law on public access to documents in the context of transparency obligations (lit. c).

The obligation of Art. 19(1)(a) is connected with and secured by the obligation in Art. 19(1(c) to erase the data as soon as they are no longer necessary for the stated purpose. Correspondingly to the obligation to inform the data holder that the data have been destroyed, the data holder should also have the right to inquire whether the data is still stored.[624] Nevertheless, rec. 73 allows the use of the data for other purposes if the data holder that made the data available has expressly agreed for the data to be used for other purposes.

According to Art. 19(2) the public sector body or a third party receiving data should not use the data they receive to develop a product or service that competes with the product or service from which the data originated nor share the data with another third party for that purpose. This provisions mirrors the obligation of the data holder in Art. 4(10).

Additionally, rec. 74 obliges the public sector body receiving data when reusing it to "respect both existing applicable legislation and contractual obligations to which the data holder is subject". This implies that contractual obligations of the data holder therefore might prevent data use on

624 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 57 n. 157.

the basis of Chapter V.[625] Such a consequence should have been regulated directly in the provisions and not merely in a recital.[626] If contractual obligations always trump the obligation to make data available, it could pose an incentive for data holders and third parties to circumvent the obligation under Art. 14.[627] A provision similiar to Art. 7(2), declaring derogation clauses non-binding would have been better suited to foster B2G data sharing.[628] The recital also goes further than and even seems to contradict Art. 17(1)(j) which only requires the public sector body to "make its best efforts to avoid compliance with the data request resulting in the data holders's liability for infringement of Union or national law".

According to Art. 19(3) and rec. 74 the disclosure of trade secrets of the data holder to public sector bodies should only be required where it is strictly necessary to fulfil the purpose for which the data has been requested and confidentiality of such disclosure should be ensured to the data holder. The appropriate measures include the use of model contractual terms, technical standards and the application of codes of conduct. It has been suggested that technical and organisational measures could follow the approach of Art. 25 GDPR.[629]

According to Art. 19(4) a public sector body should be responsible for the security of the data it receives.

8. Compensation in Cases of Exceptional Need (Art. 20)

Whether the data holder may claim compensation depends on the kind of exceptional need which motivates the request.[630] Where the data is made

625 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 59 n. 162.

626 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 59 n. 162.

627 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 59 n. 162.

628 Cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 59 n. 162; Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 73.

629 Schröder, M., *MMR-Beil.* 2024, 104 (108); Specht-Riemenschneider *MMR-Beil.* 2022, 809 (825).

630 Various actors proposed that an adequate compensation mechanism should be implemented for all scenarios of an exceptional need that require the making available of data, see Leistner, M. / Antoine, L., IPR and the use of open data and data sharing

available to respond to a public emergency pursuant to Art. 15(a), according to Art. 20(1), the data holder should provide the data free of charge, as the safeguarding of a significant good is at stake in such cases, rec. 75. Rec. 75 gives further reason in this regard: "Public emergencies are rare events and not all such emergencies require the use of data held by enterprises. [...] The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies having recourse to [the Data Act]." However, it is also argued that precisely the exceptional character of data requests in cases of public emergencies are the reason why data holders should be compensated.[631]

In other cases of exceptional need pursuant to Art. 15(b), the data holder should be entitled to fair remuneration as these cases might be more frequent, rec. 75. According to Art. 20(4), however, data holders cannot request compensation in cases of Art. 15(b), if the specific task is the production of official statistics and where the purchase of data is not allowed by national law. The member states should notify the commission about such laws (Art. 20(4) sent. 2).

Rec. 75 clarifies that the compensation should not be understood as constituting payment for the data itself and as being compulsory. According to Art. 20(2) such compensation shall cover the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, plus a reasonable margin. The data holder should provide information on the basis for the calculation of the costs and the reasonable margin upon request of the public sector body. The public sector body can request that the data holder provides information on the basis for the calculation of the costs and the reasonable margin. It is neither clearly defined nor further elaborated in the recitals what a "reasonable margin" is and how it should be calculated, thus leading to legal uncertainty.

As the obligation to provide data might constitute a considerable burden on microenterprises and small enterprises (rec. 75), Art. 20(2) applies to small and micro enterprises in all scenarios, even in cases of public emergencies, Art. 20(1), (3).

initiatives by public and private actors, 2022, p. 111; Perarnaud, C. / Fanni, R., The EU Data Act – Towards a new European data revolution?, 2022, p. 4.

631 Höne, M. / Knapp, J., *ZGI* 2023, 168 (171).

In case the public sector body disagrees with the requested level of compensation, it may submit a complaint to the competent authority of the member state where the data holder is established, Art. 20(5).

9. Contribution of Research Organisations or Statistical Bodies (Art. 21)

Art. 21(1) entitles the public sector body to share data received under Chapter V with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested (lit. a). It may also share the data with national statistical institutes and Eurostat for the compilation of official statistics (lit. b), if compatible with the purpose for which the data was requested. Regarding the meaning of "compatible with the purpose" of the request, it remains open how strict it should be interpreted especially concerning its link to the specific emergency.[632]

In such cases, the public sector body should notify the data holder from whom the data was received without undue delay, Art. 21(5). The notification should state the identity and contact details of the organisation or the individual receiving the data, the purpose of the transmission or making available of the data, the period for which the data will be used and the technical and organisational protection measures taken, including where personal data or trade secrets are involved. Where the data holder disagrees with the transmission or making available of data, it may lodge a complaint with the competent authority referred to in Art. 37 of the member state where the data holder is established.

The individuals or organisations receiving the data pursuant to Art. 21(1) should act either on a not-for-profit basis or in the context of a public-interest mission recognised in Union or member state law, not including organisations on which commercial undertakings have a significant influence which is likely to result in preferential access to the results of the research, Art. 21(2) and rec. 76. This resembles Art. 18(c) DGA which requires data altruism organisations to operate on a not-for-profit basis. The individuals or organisations receiving the data must also comply with the provisions of Art. 17(3) and Art. 19.

632 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 57 n. 156; Schröder, M., *MMR-Beil.* 2024, 104 (107).

According to Art. 21(4) and notwithstanding Art. 19(1)(c) individuals and organisations within the scope of Art. 21(1) may keep the data received for up to 6 months following the erasure of the data by the public sector bodies.

The data sharing for research purposes allows for data sharing with individuals and organisations working on a non-profit basis. This ignores that also profit based research is valuable and often essential in cases of public emergencies, as proven during the pandemic.[633] The provisions on data sharing for scientific purposes are therefore not fully sufficient to enable effective research.[634]

However, according to rec. 63 research-performing organisations and research-funding organisations organised as public sector bodies or as bodies governed by public law already have access rights under Art. 14 and 15. Consequently, for research organisations governed by public law Art. 14 and 15 might even be more relevant than Art. 21. Generally, it is nevertheless an advantage that Art. 21-actors might not have to file a request by themselves, but receive data 'through' another public sector body.

10. Mutual Assistance and Cross-Border Cooperation (Art. 22)

Art. 22(1) obliges the public sector bodies and Union institutions, agencies, and bodies to cooperate and assist one another in order to implement Chapter V in a consistent manner. The following paragraphs (Art. 22(2) to (4)) clarify the preconditions of this assistance. Especially, the exchanged data may not be used in a manner incompatible with the purpose for which they were requested, Art. 22(2).

Art. 22(3) and (4) regulate the procedure in cases, in which the requesting eligible body and the data holder are not in the same member state or the request comes from a Union body. Union bodies as well as public sector bodies intending to request data from a data holder established in another member state should first notify the competent authority of that member state as referred to in Art. 37 (Art. 22(3)).

The competent authority should evaluate the request. The competent authority should examine the request in light of the requirements under Art. 17 and take one of the actions laid down in Art. 22(4)(a)-(b). It should either

633 Specht-Riemenschneider, L., *MMR-Beil. 2022*, 809 (826).
634 Specht-Riemenschneider, L., *MMR-Beil. 2022*, 809 (826).

- transmit the request to the data holder and advise the requesting public sector body, the Commission, the European Central Bank or Union body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request (lit. a); or
- alternatively, reject the request on duly substantiated grounds in accordance with Chapter V (lit. b).

The requesting public sector body should take into account the advice of and the grounds provided by the relevant competent authority before taking any further action such as resubmitting the request (Art. 22(4)). The competent authority should act without undue delay, Art. 22(4).

This structure parallels the approach followed by the GDPR. Therefore, the challenges and difficulties of establishing the cooperation structure according to Art. 60-62 GDPR might also be paralleled in the cooperation mechanism of the Data Act.[635]

In cases of a challenge according to Art. 18(5) it is unclear in which member state they should be brought before a competent authority and which possibility to challenge or complain the requesting body has in cases where either the data holder declines the request or the competent authority rejects it.[636]

11. Interplay with Art. 6 GDPR

While the request should as far as it is possible be limited to non-personal data, Art. 17(2)(e), and only include personal data where strictly necessary (rec. 72), cases of exceptional need might often necessitate a request concerning also personal data. Personal data, however, only falls in the scope of the request in cases of Art. 15(1)(a)

635 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 111.

636 Schröder, M., *MMR-Beil.* 2024, 104 (107).

Relationship between Art. 15 and Art. 6 GDPR

As far as personal data is concerned, the making available of data according to Art. 14 and 15 would require a legal basis according to Art. 6 GDPR – as the Data Act is without prejudice to the GDPR (Art. 1(5)). However, Art. 1(5) leaves room for interpretation whether a potential legal basis according Art. 6 GDPR can be established by the Data Act. Some commentators interpret Art. 1(5) in such a way as precluding that the provisions of Chapter V constitute a legal basis according to Art. 6(1)(e), (3) GDPR.[637] Nevertheless, as Art. 6(1)(c), (e) GDPR already provides the possibility of a legal basis outside the GDPR, this would not create a conflict between the GDPR and the Data Act, as it actually complies with the provisions of the GDPR. Rec. 69 also provides that in "accordance with Article 6(1) and 6(3) of Regulation (EU) 2016/679 … when providing for the legal basis for the making available of data by data holders, in cases of exceptional needs", clarifying that Chapter V should be understood as a legal basis in Union law for the processing of personal data according to Art. 6(1)(e), (c) and Art. 6(3) GDPR. Concurringly, *Leistner* and *Antoine* also argue that the GDPR itself provides the respective legal basis in Art. 6(1)(d) and (e) as situations of exceptional need as defined in Art. 15 will often also justify a need for personal data.[638] However, the threshold of Art. 6(1)(d) is high and cannot be assumed for any case of exceptional need but would have to be proven for each request.

Art. 6(1)(e) GDPR could justify that the public sector body receives and uses personal data, but needs a legal basis outside of the GDPR, Art. 6(3) GDPR. This legal basis could be the provisions of Chapter V, if they meet the requirements of Art. 6(3) GDPR. As a legal basis according to Art. 6(1)(e) GDPR it must either state the purpose of the data processing or the purpose should be necessary for the performance of a task carried out in the public interest, Art. 6(3) GDPR. Art. 14, 15(1)(a) state the aim of the data processing as combatting a public emergency. Art. 6(3) GDPR also requires that the legal basis meets an objective of public interest and be proportionate to the legitimate aim pursued. Art.15(1)(a) meets an objective of public interest. The processing of personal data is proportionate to the aim of

637 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (669).

638 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 111.

combatting public emergencies, Art. 15(1)(a), especially since it should be anonymised or pseudonymised were possible, Art. 18(4).

The data holder who makes personal data available based on a request under Art. 14 could be justified according to Art. 6(1)(c) GDPR, as it is necessary for compliance with a legal obligation.[639] According to Art. 6(1)(c), (3) GDPR it would need to determine the aim of the data processing it requires, Art. 6(3) GDPR, as Art. 14, 15(1)(a) do. However, it could also be argued that a separate justification for the data holder making the data available is not needed, as it could be seen as a specification under Art. 6(3) from whom the public sector body can request the data.

Under Art. 15(c) in the draft Data Act, data processing would have been allowed for various undetermined purposes. The significance of these tasks varied and not each task in the public interest would have justified the processing of any kind of personal data and also the extent of protection needed for different kinds of personal data.[640] Thus, it is understandable, that the corresponding Art.15(1)(b) of the final Data Act only applies to non-personal data. However, it also includes cases of preventing a public emergency, which could justify the making available of personal data and are similar to cases of combatting public emergencies and thus should have been included in Art. 15(1)(a).[641]

In the following articles, especially in Art. 18-21, the Data Act contains specific provisions to adapt the application of rules of the GDPR, as allowed in Art. 6(3) GDPR.

Relationship between Art. 18(5) and Art. 6 GDPR

It is also debated whether Art. 18(5) stipulates a legal ground for data processing according to Art. 6(1)(c) GDPR, as anonymisation and pseud-

639 See also Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, pp. 57 et seq.

640 Cf. Wienroeder, M, 2022, Part II (Art. 14-22), in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (ed.), The Data Act Proposal – Literature Review and Critical Analysis, University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-02, p. 25.

641 Cf. Wienroeder, M, 2022, Part II (Art. 14-22), in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (ed.), The Data Act Proposal – Literature Review and Critical Analysis, University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-02, p. 25.

onymisation constitute data processing under Art. 4(2) GDPR.[642] In the context of chapter V, Art. 18(5) has to be seen as a specific provision within the legal basis according to Art. 6(1)(c), (e), (3) GDPR adapting the application of rules of the GDPR on "processing operations and processing procedures" (see above). Thus, no further legal ground for the anonymisation and pseudonymisation of the requested data is needed.

Relationship between Art. 21 and Art. 6 GDPR

Regarding Art. 21 it is questionable whether it needs its own justification under Art. 6(1) or also falls under the specification according to Art. 6(3) GDPR, more specifically as a specification on "the entities to, and the purposes for which, the personal data may be disclosed". As the aim of data sharing for research purposes under Art. 21 is not only the disclosure of data but also further data processing by the research organisation, it is questionable whether this should be encompassed as a specification according to Art. 6(3) GDPR. Still, the purpose of data disclosure to other entities will usually be data processing in some form. So, Art. 6(3) could also be interpreted as allowing for provisions on data sharing such as Art. 21.

12. Legal Remedies and Liability

Chapter V provides the possibility to lodge a complaint with the competent authority designated pursuant to Art. 37 in the cases of disputes whether the conditions laid down in Art. 17 are met or over the decline of the request (Art. 18(5)), when the data holders rights under Chapter V have been infringed by the transmission or making available of data according to Art. 17(5), in cases of disputes over the amount of compensation (Art. 20(5)), or in cases of making data available to research organisations and statistical bodies according to Art. 21(5). Those provisions lack clarification with regard to the respective procedure, their legal nature, and their legal effects. Especially, the framework for interim proceedings and the legal protection in cross-border cases could have been further clarified.[643]

642 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 58 n. 160.

643 Schröder, M., *MMR-Beil.* 2024, 104 (108).

Additionally, Art. 19(4) provides that the requesting bodies should be responsible for the security of the data they receive, without providing legal consequences when the responsibility is violated. It does not seem to entail an independent legal claim for the data holder.[644] However, a violation could be claimed through a complaint according to Art. 17(5).

644 Schröder, M., *MMR-Beil.* 2024, 104 (108).