# X. International Governmental Access and Transfer (Art. 32)

Chapter VII ('Unlawful International Governmental Access and Transfer of Non-Personal Data', Art. 32) aims to prevent unlawful governmental access to non-personal data held in the Union by data processing services offered on the Union market through technical, legal, and organisational safeguards.[862] Rec. 101 argues respectively that "third countries may adopt laws, regulations and other legal acts that aim to directly transfer or provide governmental access to non-personal data located outside their borders, including in the Union."

The provision of Art. 32 recalls similar provisions first in the GDPR (Art. 44-50) for personal data and then in the DGA (Art. 31); the latter being concerned with non-personal data as well as with data sharing services, public sector bodies, natural or legal persons with the right to re-use data and recognised data altruism organisations. Generally, the structure and provisions of Art. 32 mirror the approach of Art. 31 DGA, with few differences.

The terms "access" and "transfer" are not defined in the Data Act. As Art. 32 uses the same wording as Art. 31 DGA and mirrors its provisions, it seems plausible to also apply the definition in Art. 2(13) DGA for "access" as meaning "data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data". While neither the Data Act nor the DGA define "transfer", it still seems plausible to understand it similarly. For Art. 31 DGA it is argued to understand "transfer" in contrast to the definition of "access" as only meaning the active disclosure of data to third-countries.[863]

Art. 32 only addresses data held by data processing services according to Art. 2(12).[864] Thus, other activities of a company that is not only active as a

862 Commission, COM(2022) 68 final Explanatory Memorandum, p. 16.

863 Hennemann, M., in: Specht-Riemenschneider, L./Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 32; Schreiber, K. / Pommerening, P. / Schoel, P., Das neue Recht der Daten-Governance, § 5 mn 6 et seq.

864 The broad term "providers of data processing services" also includes cloud storage providers, thus leading to an efficient protection of data which is not stored in in-house infrastructure, see Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 115.

data processing service are not covered by Art. 32.[865] They might, however, fall under the scope of the GDPR or the DGA (Art. 31).

According to Art. 32 and as a general rule, the transfer of non-personal data is generally allowed and partially regulated by Art. 32 (while the transfer of personal data is according to Art. 44-50 GDPR generally forbidden and only in specific cases allowed).[866] In practice, however, it might become difficult to determine whether Art. 44-50 GDPR or Art. 32 apply, as firstly personal and non-personal data may be mixed in datasets and secondly it is increasingly hard to distinguish personal and non-personal data.[867]

Generally, the approach of Art. 32 is not free of doubt. There is the risk that it hinders the objectives of Art. 23-31 to enable switching between data processing services, which means a transfer of data, by obliging the providers of data processing services to prevent international governmental access and transfer. It is therefore questioned whether Art. 32 is in line with the principal objective of the Data Act to enhance data sharing.[868] Some commentators have advocated that Art. 32 is not necessary and justified as – with regard to non-personal data – its prime objective is not the protection of fundamental rights and freedoms of the data subject.[869] However, non-personal data can have implications for the public interest, for example related to trade secrets, intellectual property, and public security that can justify the restriction of international data transfer.

### *1. Preventing International and Third-Country Governmental Access and Transfer of Non-Personal Data (Art. 32(1))*

Where a governmental access or transfer would create a conflict with Union law or the national law of the relevant member state, Art. 32(1) obliges the providers of data processing services to take all adequate technical, legal, and organisational measures, including contracts, in order to prevent

865 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 189.

866 Hennemann, M., in: Specht-Riemenschneider, L./Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 1.

867 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 69.

868 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 189.

869 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 190.

international and third-country governmental access and transfer of such non-personal data held in the Union.

The MPIIC argued concerning the provision of the draft Data Act, that it could lead to data processing service providers completely refraining from transferring data to countries outside of the EU.[870] According to its interpretation of the provision of the draft Data Act it could have required the monitoring of the content of all data, although a provider of data processing services is not a content provider.[871] Insofar, the wording of the final provision indicates more clearly that only governmental access and transfer and not any international transfer creating a conflict with union law should be prevented. Still as no specific event as for example a judgement is required (as in paragraph (2) and (3)),[872] the requirement to take all reasonable measures to prevent any governmental access or transfer creating a conflict with union law is a considerable burden on providers of data processing services.

The assessment of this provision depends in particular on the understanding of "create a conflict with union law". The MPIIC interprets it as even requiring less than an actual violation of the law by the data access or transfer.[873] Also, a different interpretation of Art. 32(1) seems possible. One might argue that that the transfer shall only be restricted in specific cases where legislation specifically prohibits governmental access or transfer.[874] In light of the final wording of the provision this interpretation seems more plausible. Potentially along these lines, rec. 101 specifies such potential conflicts with Union or member state law as conflicts with obligation to protect such data, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to an effective remedy, or the fundamental interests of a member state related to national security or defence, as well as the protection of commercially

870 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 197.

871 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 200.

872 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 198 et seq.

873 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

874 See also in the context of the parallel rule of Art. 31 DGA Hennemann, M., in: Specht-Riemenschneider, L./Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 24.

sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law. The obligation to prevent governmental access to and transfer of non-personal data should thus not be understood as an independent liability provision for the data processing services.[875]

The draft Data Act followed the wording of the DGA and required providers of data processing services to take all "reasonable [...] measures", while the final wording differs from the DGA, requiring "adequate [...] measures". While both have a similar meaning, the deliberate deviation from the wording of Art. 31 DGA indicates that indeed a different standard is required. In rec. 102 "the encryption of data, the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies" are given as exemplary measures that should be taken by the providers of data processing services.

### *2. Enforcement of Foreign Judgements and Decisions (Art. 32 paras. 2 and 3)*

Judgments of third-country courts or tribunals or decisions of third-country administrative authorities, including law enforcement authorities requiring such transfer or giving access to non-personal data should only be recognised or enforceable when based on an international agreement, such as a mutual legal assistance treaty[876], in force between the requesting third country and the Union or a member state, Art. 32(2) and rec. 101. If such an agreement exists, it sets a clear legal standard.[877] Rec. 101 further explains that

> "in other cases, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law conflicts with an obligation to protect such data under Union law or under the national law of the relevant Member State, in particular regarding

875 See in the context of the parallel rule of Art. 31 DGA Hennemann, M., in: Specht-Riemenschneider, L. / Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 40.

876 For example the Agreement on mutual legal assistance between the European Union and the United States of America (2003) or the Agreement between the European Union and Japan on mutual legal assistance in criminal matters (2010).

877 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 70 n. 193.

the protection of fundamental rights of the individual, such as the right to security and the right to an effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, including its contractual undertakings regarding confidentiality in accordance with such law."

In the absence of international agreements regulating such matters and if compliance with the decision would risk putting the addressee in conflict with Union law or the relevant national law, transfer or access should only be allowed according to Art. 32(3), if

(a) the third-country system requires the reasons and proportionality of such a decision or judgement to be set out and requires such a decision or judgement to be specific in character (…); and
(b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and
(c) the competent third-country court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected by Union law or by the national law of the relevant Member State.

Art. 32(3) regulates in particular scenarios in which the data processing service is in a conflict of contradictory duties according to different legal systems.[878] To determine, whether the conditions laid down in the first subparagraph are met, according to Art. 32(3)(2) the addressee of the decision can ask the opinion of the relevant national body or authority competent for international cooperation in legal matters, notably when it considers that the decision may relate to trade secrets and other commercially sensitive data as well as to content protected by intellectual property rights or the transfer may lead to re-identification. This mitigates the burden on the service provider.[879] If the addressee considers that the decision may impinge on national security or defence interests of the Union or its member states,

878 See in the context of the parallel rule of Art. 31 DGA Hennemann, M., in: Specht-Riemenschneider, L. / Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 53.

879 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 71 n. 194.

it shall ask the opinion of the national competent bodies or authorities with the relevant competence, in order to determine whether the data requested concerns national security or defence interests of the Union or its member states, Art. 32(3) subpara. 2 sent. 2. If the addressee has not received a reply within a month, or if the opinion of the competent authorities concludes that the conditions are not met, the addressee may deny the request for transfer or access on those grounds, Art. 32(3) subpara. 2 sent. 3. The wording of this subparagraph clarifies that the determination whether there is a conflict with EU or national law according to Art. 32(1) is not covered in its provisions,[880] although also in this scenario the possibility to ask the opinion of the national competent bodies would have helped foster legal certainty for data processing services.

The wording "may reject" implies that the issued opinions of the competent authorities are not binding, as the addressee of the decision is not obliged to deny the transfer of data. It is however questionable that the case of not receiving a reply should be treated the same as when the conditions of the first subparagraph are not met.

The EDIB shall advise the Commission on developing guidelines on the assessment of whether the conditions laid down in Art. 32(3) are met.[881]

*Leistner* and *Antoine* see the conditions for transferring or making data available laid down in Art. 32(3) as an adequate and structured framework for protecting non-personal data against inadequate international transfer or governmental access.[882] In contrast, the BDI criticises, that it implements a level of protection for non-personal data which is usually only known for the protection of personal data as protection of fundamental rights.[883]

### *3. Minimisation and Informational Duty (Art. 32 (4) and (5))*

According to Art. 32(4), "if the conditions laid down in para. 2 and 3 are met, the provider of data processing services shall provide the minimum

880 This was less clear under the original proposal, cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 71 n. 195.

881 Welcomed bv Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 116; BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 21.

882 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 115.

883 BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 21.

amount of data permissible in response to a request". The "minimum amount of data" should be determined based on either the provider's reasonable interpretation of the request or that of the relevant competent body's or authority's, Art. 32(4). Referring to the "amount of data" is rather misguided, as often the informational content is more important than its amount.[884]

The rule of Art. 32(4) applies if the transfer of non-personal data is not in conflict with Union law or the national law of the relevant member state. If such a conflict exists the data should not be transferred.[885]

The provision refers to the reasonable interpretation of the respective request by the relevant national body or authority referred to in Art. 32(3) and (2). This approach does not really clarify this vague requirement, which was already criticised in the parallel Art. 31(4) DGA[886].

According to Art. 32(5) the provider of data processing services should inform the customer about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity. Rec. 101 adds, that the provider of data processing services should,

> "wherever possible under the terms of the data access request of the third country's authority, be able to inform the customer whose data are being requested before granting access to those data in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality."

884 Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 72 n. 196.

885 See in the context of the parallel rule of Art. 31 DGA Hennemann, M., in: Specht-Riemenschneider, L. / Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 60.

886 Hennemann, M., in: Specht-Riemenschneider, L. / Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, mn. 59.