ERA Forum (2021) 22:541–556
https://doi.org/10.1007/s12027-021-00679-1

ARTICLE

Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations

Xavier Tracol [1]

Accepted: 19 July 2021 / Published online: 4 August 2021

Abstract

Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies shows that its general principles, approach, architecture and legal bases are all consistent with those provided for in both the General Data Protection Regulation and the Law Enforcement Directive. The *Schrems* II judgment has far-reaching implications for Union institutions and bodies. The extremely limited number of adequacy decisions shows the practical importance of appropriate safeguards as a legal basis for Union institutions and bodies to transfer personal data to third states and international organisations. In this context, the availability of updated standard contractual clauses is a welcome development.

Keywords Regulation (EU) 2018/1725 · Union institutions and bodies · Chapter V · Transfers · Personal data · Third states · International organisations · *Schrems* II judgment · UK · Brexit

The views expressed herein are those of the author in his personal capacity and do not necessarily reflect those of EUROJUST or the EU in general. The author warmly thanks Ms Diana Alonso Blas, Data Protection Officer and Head of the Data Protection Service at Eurojust, for her thorough proof reading and constructive comments on a draft of this article.

✉ X. Tracol Ph.D
xtracol@eurojust.europa.eu

[1] Senior Legal Officer, Data Protection Office, EUROJUST, P.O. Box 16183, 2500 BD, The Hague, The Netherlands

1 Introduction

Chapter V of Regulation (EU) 2018/1725[1] ("the Regulation") applies to transfers by Union institutions and bodies understood as "Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty" (Art. 3(10) thereof) of personal data to third states and international organisations. This publication will first analyse the scope of Chapter V of the Regulation (1). It will then analyse the general principles which apply to transfers, the approach of Chapter V of the Regulation, the architecture of transfers and the implications of the judgment rendered by the Grand Chamber on 16 July 2020 in the *Schrems* II case ("*Schrems* II judgment")[2] (2). The available legal bases of transfers will ultimately be analysed (3).

2 Scope

Personal data is defined in Art. 3(1) of the Regulation as "any information relating to an identified or identifiable natural person". This broad definition therefore encompasses all personal data processed by Union institutions and bodies in the context of their specific mandates where they carry out tasks in the public interest entrusted to them by EU law. Evidence is available that the number of transfers related to the core business of Union institutions and bodies doubled over the last few years.[3]

The scope of Chapter V of the Regulation also includes "administrative personal data, such as staff data" as mentioned in Recital 14 thereof. The personal data of staff members certainly represents a large portion of administrative personal data processed by all Union institutions and bodies, regardless of their different mandates.

The scope of Chapter V of the Regulation however excludes transfers by Union institutions and bodies to third states and international organisations of operational personal data. The latter phrase is defined in Art. 3(2) of the Regulation as "all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies". Chapter IX of the Regulation applies to transfers of operational personal data by Union institutions and bodies to third states and international organisations. In practice, the scope of this chapter is currently limited to both Eurojust and Frontex, pursuant to Art. 26(1) of the Eurojust Regulation[4] and Art. 90(1) of

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39 [27].

[2] C-311/18 *Facebook Ireland and Schrems*, EU:C:2020:559 [2].

[3] European Data Protection Supervisor, Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, 29.10.2020, available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf [31], p. 6 and 7.

[4] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA [2018] OJ L 295/138 [28].

the Frontex Regulation.[5] The practical scope of Chapter V is accordingly limited to administrative personal data for these two agencies. The Commission submitted a proposal to apply Chapter IX of the Regulation to Europol.[6] The Commission will also submit a proposal to apply Chapter V thereof to the European Public Prosecutor's Office to ensure a uniform and consistent level of protection, pursuant to Art. 98(2) of the Regulation.

Transfers should be clearly distinguished from other processing activities such as access and storage. In other words, transfers of personal data do not require, involve or imply access or storage. Transfer, access and storage are three different processing activities. Chapter V of the Regulation on transfers of personal data by Union institutions and bodies to third states and international organisations includes six provisions only, *i.e.* Art. 46 to 51.

3 General principles of transfers

Any transfer of personal data by Union institutions and bodies must comply with Chapter V of the Regulation *and* is subject to other provisions thereof. In addition, the application of legal bases for transfers available under Chapter V of the Regulation including derogations should not undermine the level of protection of personal data guaranteed thereby (Art. 46 and Recital 63 of the Regulation).

The *Schrems* II judgment is legally based *inter alia* on Article 7 about the respect for private life, Article 8 about the protection of personal data and Article 47 about the right to an effective remedy of the Charter of Fundamental Rights ("the Charter").[7] The latter which is part of EU primary law applies to Union institutions and bodies, pursuant to Art. 51(1) of the Charter. On 29 October 2020, the European Data Protection Supervisor (EDPS) therefore published a Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling.[8] This Strategy aims at monitoring the compliance of Union institutions and bodies with the *Schrems* II judgement on transfers of personal data to third states in general and to the United States (US) in particular. The goal is that ongoing and future international transfers be carried out in accordance with EU data protection law. In light of the factual background of the *Schrems* II judgment, the EDPS set out in its Strategy priority criteria for transfers of personal data to private entities in the US in ongoing contracts. The EDPS also developed an action plan distinguishing between

[5] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1 [29].

[6] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, 9.12.2020, COM(2020) 796 final, 2020/0349 (COD) [22].

[7] See Xavier Tracol, "*Schrems* II: the return of the Privacy Shield", *Computer Law & Security Review*, Volume 39, November 2020 [35], p. 1 to 11.

[8] [31] Available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

short-term and medium-term compliance actions. This action plan includes both a mapping exercise and a reporting exercise on specific categories of transfers. It also cautions for future services and new processing operations and requests that Union institutions and bodies carry out case-by-case transfer impact assessments to evaluate whether the third state of destination provides an essentially equivalent level of protection as in the European Economic Area (EEA). Union institutions and bodies should pay particular attention to *onward transfers* of personal data by recipients in third states to third parties such as sub-processors and sub-contractors in the same or another third state. Art. 46 of the Regulation clearly provides that all requirements set out in Chapter V of the Regulation equally apply to onward transfers. Union institutions and bodies must accordingly comply with such requirements, which is even more important since onward transfers may involve multiple recipients.

In line with its Strategy, the EDPS issued an order to Union institutions and bodies on 5 October 2020 for them to complete a mapping exercise identifying which ongoing contracts, procurement procedures and other types of cooperation involve transfers of personal data to third states. The EDPS requested Union institutions and bodies to report to it about transfers without any legal basis, transfers based on derogations and transfers to private entities towards the US presenting high risks for data subjects. Regarding new processing operations or new contracts with service providers, the EDPS strongly encouraged Union institutions and bodies to avoid processing activities which involve transfers of personal data to the US. The EDPS's analysis of the outcome of this mapping exercise unsurprisingly shows that personal data is transferred to third states in general and to the US in particular, especially when Union institutions and bodies use tools and services offered by large service providers. The analysis of the EDPS also shows that Union institutions and bodies increasingly rely on cloud-based software and cloud infrastructure or platform services from large ICT providers. Some providers are located in the US and therefore subject to legislation which allows disproportionate surveillance activities by US authorities, according to the *Schrems* II judgement.

On 27 May 2021, the EDPS launched two investigations as part of its Strategy so that ongoing and future transfers of personal data to third states are carried out in accordance with EU data protection law. The first investigation deals with the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by Union institutions and bodies. The second investigation deals with the use of Microsoft Office 365 including Microsoft Teams by the Commission.[9]

The approach of Chapter V of the Regulation about the architecture of transfers is that Union institutions and bodies as controllers or processors may first transfer personal data to third states and international organisations where the Commission has issued an *adequacy decision*. In the absence of any adequacy decision, Union institutions and bodies may transfer personal data to third states and international organisations subject to *appropriate safeguards*. In the absence of any adequacy decision or appropriate safeguards, Union institutions and bodies may transfer personal data to third states and international organisations on the basis of *derogations for*

[9] See press release EDPS/2021/11, "The EDPS opens two investigations following the 'Schrems II' Judgement", 27.5.2021 [21], available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

specific situations. Derogations are however an option of last resort to which Union institutions and bodies should make recourse with extreme care in exceptional cases and for occasional transfers only.

The approach of Chapter V of the Regulation is therefore flexible. If an adequacy decision of the Commission is available, Union institutions and bodies do not need to consider appropriate safeguards. If appropriate safeguards are provided, Union institutions and bodies do not need to consider derogations. The architecture of applicable provisions on transfers of personal data by Union institutions and bodies to third states and international organisations under Chapter V of the Regulation is similar to both the architecture of applicable provisions on transfers of personal data to third states and international organisations under Chapter V of the General Data Protection Regulation[10] (GDPR) and the architecture of applicable provisions on transfers of operational personal data to third states and international organisations under Chapter V of the Law Enforcement Directive.[11]

4 Legal bases of transfers

Transfers of personal data by Union institutions and bodies to third states and international organisations may be legally based on an adequacy decision (3.1), appropriate safeguards (3.2) or derogations for specific situations (3.3). Art. 31(1)(e) and Art. 31(2)(c) of the Regulation provide for the obligation of each controller and processor to maintain a *record of processing activities*. This record must contain all the information about transfers of personal data to third states and international organisations including the identification of such states and organisations and the documentation of suitable safeguards.

Where a controller intends to transfer personal data to a third state or an international organisation, Art. 15(1)(e) and Art. 16(1)(f) of the Regulation both set out that this controller must provide data subjects with information about the existence or absence of an adequacy decision by the Commission, or in the case of transfers subject to appropriate safeguards, "reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available." Last but not least, Art. 66(3)(c) of the Regulation provides that infringements upon transfers by Union institutions or bodies of personal data to a recipient in a third state or an international organisation pursuant to Art. 46 to 50 of the Regulation are subject to administrative fines of up to € 50,000 per infringement and up to a total of € 500,000 per year.

[10]Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/89 [26].

[11]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, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 [11].

4.1 Transfers based on an adequacy decision

Art. 47(1) of the Regulation provides for two cumulative requirements, *i.e.* a "transfer of personal data to a third country or international organisation may take place":

(1) where the Commission has issued an adequacy decision *and*

(2) "where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out."

Art. 47 of the Regulation on adequacy decisions refers to decisions of the Commission under *either the GDPR or the Law Enforcement Directive*. Two alternative legal bases are accordingly available. In practice, Union institutions and bodies will presumably rely on an adequacy decision based on the Law Enforcement Directive to transfer personal data to a third state or international organisation only in the unlikely situation where the Commission has not issued any adequacy decision based on the GDPR with the same third state or international organisation. The practical implementation for Union institutions and bodies to transfer personal data to a third state or international organisation pursuant to an adequacy decision based on the Law Enforcement Directive remains to be clarified.

Chapter V of the Regulation does however not refer to international agreements concluded by the EU and a third state or an international organisation, pursuant to Art. 218 of the TFEU. The latter requires the consent of Parliament unlike adequacy decisions in which the Commission alone has the power to decide that a third state or international organisation ensures an adequate level of protection.[12]

Art. 47 of the Regulation cross-refers to the applicable standard of *adequate level of protection* set out in both Art. 45 of the GDPR and Art. 36 of the Law Enforcement Directive about transfers on the basis of an adequacy decision.

The *scope of the adequacy decision* may be limited to "a territory or one or more specified sectors" within the third state. The decision does accordingly not need to apply to the third state as a whole.

In practice, the Commission has issued two adequacy decisions based on the GDPR so far about Japan on 23 January 2019[13] and about the United Kingdom (UK) on 28 June 2021.[14] That same day, it issued the first adequacy decision based on the Law Enforcement Directive about the UK.[15] The two decisions on the UK entered

[12] See Xavier Tracol, "Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada", *Computer Law & Security Review*, Volume 34, issue 4, August 2018 [34], p. 840, para. 6.2.

[13] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76/1 [3].

[14] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom [5], available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en.

[15] Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final [6], available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en.

into force on 28 June 2021. Personal data can accordingly continue being transferred from the EEA to the UK. The two adequacy decisions about the UK also facilitate the correct implementation of the EU-UK Trade and Cooperation Agreement[16] which foresees the exchange of personal data, for example in the area of cooperation on judicial matters. For the first time, the decisions both include a so-called "sunset clause" which limits the duration of adequacy to four years. This provision means that the two decisions will automatically expire four years after the date when they entered into force.

Regarding the background of the two decisions, the Commission had published two draft adequacy decisions about the UK on the basis of both the GDPR[17] and the Law Enforcement Directive[18] on 19 February 2021. They both assessed whether the data protection framework of the UK provided for adequate protection of EEA citizens' personal data. On 13 April 2021, the European Data Protection Board (EDPB) published two Opinions 14/2021 and 15/2021 about the draft implementing decisions of the Commission pursuant to the GDPR and the Law Enforcement Directive on the adequate protection of personal data in the UK.[19] In its first Opinion, the EDPB focused on assessing whether the British data protection framework is aligned with the GDPR, both on the general data protection aspects and on the transfers of personal data from the EEA to the UK for law enforcement and national security purposes specifically. In its second Opinion, the EDPB focused on assessing whether the data protection framework of the UK on transfers of personal data for the prevention, investigation, detection or prosecution of criminal offences ensures an adequate protection aligned with the Law Enforcement Directive and Recommendations 01/2021 of the EDPB on the adequacy referential under the Law Enforcement Directive.[20] In the same vein, the EDPB also assessed whether the data protection framework of the UK complies with Recommendations 02/2020 of the EDPB dated 10 November 2020 on the European Essential Guarantees for surveillance measures.[21] On 21 May 2021, Parliament adopted a resolution on the adequate protection of personal data by the UK which deals with the two draft adequacy decisions of the Commission.[22] On 16

[16]Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L 149/10 [36].

[17][13] Available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf.

[18][14] Available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf. See Xavier Tracol, "The two judgments of the European Court of Justice in the four cases of *Privacy International*, *La Quadrature du Net and Others*, *French Data Network and Others* and *Ordre des Barreaux francophones et germanophone and Others*: The Grand Chamber is trying hard to square the circle of data retention", *Computer Law & Security Review*, Volume 41, April 2021 [33], p. 12 and 13, section 6.7.

[19][19] and [20] Available at https://edpb.europa.eu/other-documents_en.

[20][23] Available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en.

[21][24] Available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

[22][30] Available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html.

June 2021, representatives of Member States approved the two adequacy decisions in the context of the comitology procedure.

The availability of an adequacy decision of the Commission about a third state entails rights and obligations for Union institutions and bodies. Regarding *rights*, in case of an adequacy decision, Union institutions and bodies may transfer personal data to the relevant third state or international organisation without the need to obtain any further authorisation (Recital 64 of the Regulation).

Regarding *obligations*, Union institutions and bodies must notify both the Commission and the EDPS about transfers which are suspended or terminated if Union institutions and bodies consider that the third state or an international organisation does not ensure an adequate level of protection (Art. 47(2) of the Regulation). The Commission may then render a decision where it establishes that a third state, a territory or one or more specified sectors within a third state or an international organisation, no longer ensures an adequate level of protection. In light of the latter power of the Commission, Union institutions and bodies should check the legal validity of an adequacy decision before transferring any personal data to a third state or international organisation on this basis.

4.2 Transfers based on appropriate safeguards

Recital 65 of the Regulation sets out that in the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third state by way of appropriate safeguards for the data subject. Art. 48(1) of the Regulation provides for two cumulative requirements, *i.e.*:

(1) appropriate safeguards provided by the controller or processor and

(2) availability of enforceable data subject rights and effective legal remedies for data subjects, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third state. They should relate in particular to compliance with the general principles on personal data processing, the principles of data protection by design and by default (Recital 65 of the Regulation).

Art. 17(2) of the Regulation provides that data subjects have the fundamental right to be informed about appropriate safeguards. This right accordingly translates into the obligation of Union institutions and bodies to inform data subjects where their personal data are transferred to a third state or to an international organisation.

Two different categories of appropriate safeguards should be clearly distinguished, *i.e.*: **(1)** without requiring any specific authorisation from the EDPS (Art. 48(2) of the Regulation) or **(2)** subject to the authorisation from the EDPS (Art. 48(3) of the Regulation).

4.2.1 Transfers based on appropriate safeguards: no specific authorisation from the EDPS

Art. 48(2) of the Regulation provides for an exhaustive list of four alternative cases. The appropriate safeguards may be provided for, without requiring any specific authorisation from the EDPS, by:

(a) a *legally binding instrument with public authorities* or bodies in third states or international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for *enforceable and effective rights for data subjects* (recital 65 of the Regulation): in practice, this case requires that Union institutions and bodies sign an international agreement with public authorities or bodies in third states or international organisations;

(b) *standard data protection clauses adopted by the Commission*;

(c) *standard data protection clauses adopted by the EDPS* and approved by the Commission;

(d) where the processor is not a Union institution or body, *binding corporate rules* approved by a national supervisory authority following an opinion of the EDPB, *codes of conduct*[23] or *certification mechanisms* pursuant to Art. 46(2)(b), (e) and (f) of the GDPR.

The standard contractual clauses for transfers of personal data to third states were adopted under Directive 95/46/EC,[24] which is the ancestor of the GDPR. The Commission therefore proposed a draft implementing decision on standard contractual clauses for transfers of personal data to third states, pursuant to Art. 46(2)(c) of the GDPR.[25] This decision will eventually replace the standard contractual clauses adopted under Directive 95/46/EC, which are still in force. Such clauses have been updated to take into account the requirements of both the GDPR and the *Schrems* II judgement[26] and to better reflect the widespread use of new and more complex processing operations, which often involve multiple data importers and exports. The scope of the implementing decision is intended to include processing activities between processors and sub-processors for which the controller is an Union institution or body subject to the Regulation.

The draft standard contractual clauses however reflected the requirements of the GDPR only. In a joint Opinion 2/2021 of 14 January on these draft SCCs for transfers,[27] the EDPB and the EDPS both considered that the relevant requirements of the Regulation "should be reflected throughout the entire chain of contracts" when an

[23] On 7 July 2021, the EDPB adopted Guidelines on Codes of Conduct as a tool for transfers. The guidelines clarify the interpretation of Articles 40(2)(j) and Article 40(3) of the GDPR on transfers of personal data outside the EU. The guidelines complement EDPB Guidelines 1/2019 on codes of conduct which establish the general framework for the adoption of codes of conduct as well as the procedures and rules involved in the submission, approval and publication of codes both at national and European level.

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 [12].

[25] [15] Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[26] See Xavier Tracol, "*Schrems* II: the return of the Privacy Shield", *Computer Law & Security Review*, Volume 39, November 2020 [35], p. 1 to 11.

[27] [26] Available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en.

Union institution or body is the controller. The EDPB and the EDPS stated that "[t]his should be further clarified in the Draft Decision and Draft SCCs" (paras. 23 to 25).

On 4 June 2021, the Commission issued the draft decision and draft SCCs appended as an annex thereto.[28] They both deal with transfers of personal data to third states. Recital 8 of the draft decision shows that the Commission has taken the joint Opinion of the EDPB and the EDPS into consideration. On 7 June 2021, Commission Implementing Decision (EU) 2021/914 was published in the *Official Journal*.[29] The decision enter**ed** into force 20 days after this date, *i.e.* on 28 June 2021.

Binding corporate rules remain legally valid but need updating over time in line with the GDPR.[30]

If Union institutions and bodies consider that the domestic law of the third state infringes upon the effectiveness of the appropriate safeguards, they should identify and adopt effective supplementary measures within the meaning of the *Schrems* II judgment. Such measures may take the shape of a strong and secure encryption both at rest and in transit of all personal data before any transfer thereof by Union institutions and bodies to the relevant third state.[31]

4.2.2 Transfers based on appropriate safeguards: specific authorisation from the EDPS

Union institutions and bodies must first confer with the EDPS and obtain its authorisation to rely on Art. 48(3) of the Regulation. This provision sets out a non-exhaustive list of two alternative cases.

Subject to the authorisation from the EDPS, the appropriate safeguards may also be provided for, *in particular*, by *either*:

(a) drafting *ad hoc contractual clauses* between **(1)** the Union institution or body as controller or processor and **(2)** the controller, processor or the recipient of the personal data in the third state or international organisation; *or*

(b) inserting provisions into *non legally binding administrative arrangements* between public authorities or bodies which include *enforceable and effective data subject rights* (Recital 65 of the Regulation).

On 12 May 2021, the EDPS issued its first Decision[32] on the use of an administrative arrangement as a tool which provides appropriate safeguards for the transfer of

[28] Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

[29] OJ L 199/31.

[30] Regarding binding corporate rules, see Xavier Tracol, "'Invalidator' strikes back: The harbour has never been safe, *Computer Law & Security Review*, Volume 32, issue 2, April 2016 [32], p. 359.

[31] See EDPS, Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, 29 October 2020 [31], available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

[32] EDPS Decision authorising, subject to conditions, the use of the administrative arrangement between the European Commission and the Turkish Medicines and Medical Devices Agency in the context of the Turkish participation in the EU regulatory system for medical devices Eudamed (Case 2021-0347), 12 May 2021 [17], available at https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/edps-decision-authorising_en.

personal data to third states. This arrangement deals with transfers of personal data between the Commission and the Turkish Medicines and Medical Devices Agency (TMMDA). The context of this arrangement is the Turkish participation in the EU regulatory system for medical devices, EUDAMED, which is a system for the coordination of information on medical devices available in the EU.

In its Decision, the EDPS assessed whether the arrangement provides sufficient guarantees to ensure that personal data transferred outside the EEA benefits from an essentially equivalent level of protection as in the EEA. In light of the similarities between the Regulation and the GDPR, the EDPS based its assessment on the Guidelines of the EDPB for transfers of personal data between EEA and non-EEA public authorities and bodies.[33] These Guidelines set out the criteria of the minimum data protection safeguards for inclusion in the arrangement.

In its Decision, the EDPS considered general principles relating to processing of personal data that it regarded as providing sufficient data protection safeguards to ensure an essentially equivalent level of protection as in the EEA. Such principles included purpose limitation, data accuracy, data minimisation and storage limitation.

As a result of its assessment, the EDPS recommended in its Decision that the Commission amend the following provisions of the arrangement to ensure that personal data is appropriately safeguarded:

- the purpose for which personal data may be processed;
- transparent information on how, what, why and for how long personal data may be processed;
- the provision of information to data subjects about their fundamental rights;
- security and confidentiality measures about the time when personal data may be processed;
- redress, *i.e.* which options are available to data subjects if their data is not adequately protected;
- oversight of the processing operations of personal data.

Regarding the possible access to personal data by national security or law enforcement authorities, the EDPS reiterated that the Commission—as data exporter—is responsible for seeking and assessing whether the authorities in Turkey—as data importer—provide sufficient data protection safeguards. The EDPS also advised the Commission to keep records of the laws in force in Turkey which govern the sharing of personal data with other public bodies, including for surveillance purposes. These records should be communicated to the EDPS within six months after the date of the EDPS Decision.

The EDPS requested the Commission to report on the implementation of the Decision on an annual basis. Last, the Commission should inform the EDPS without undue delay about any suspended transfers of personal data or any revision or termination of the arrangement with the TMMDA.

Art. 48(4) of the Regulation is a transitional provision. Authorisations by the EDPS on the basis of Art. 9(7) on transfer of personal data to recipients, other than

[33] EDPB Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020 [16].

Union institutions and bodies, which are not subject to Directive 95/46 of Regulation 45/2001[34] shall remain valid until amended, replaced or repealed, if necessary, by the EDPS. Art. 9(7) of Regulation 45/2001 provides that the EDPS "may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection [...], where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses."

Pursuant to Art. 9(7) of Regulation 45/2001, the EDPS rendered four authorisation Decisions for transfers *of personal data* which are all published on his Internet site:[35]

(**1**) the oldest Decision of 13 February 2014 deals with transfers carried out by OLAF through the Investigative Data Consultation Platform;[36]

(**2**) Decision of 3 June 2016: transfers by the European Central Bank for its supervisory activities;[37]

(**3**) Decision of 17 January 2018: transfers by the European Centre for Disease Prevention and Control (ECDC) to the World Health Organization (WHO);[38] and

(**4**) Decision of 13 March 2019: use of the Administrative Arrangement by the European Securities and Markets Authority.[39]

The scope of the third Decision includes transfers of personal data by the ECDC to the WHO in the specific context of the COVID-19 pandemic.

4.3 Transfers based on derogations for specific situations

Art. 50(1) of the Regulation provides that in the absence of an adequacy decision or appropriate safeguards, a transfer or a set of transfers of personal data to a third state or an international organisation must take place only on one of the 7 following alternative conditions, *i.e.*:

(1) the data subject has *explicit*ly *consent*ed to the proposed transfer, after having been informed of the possible *risks* of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

[34] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1 [25].

[35] Available at https://edps.europa.eu/data-protection/our-work/our-work-by-type/authorisation-decisions-transfers_en.

[36] [7] Available at https://edps.europa.eu/sites/default/files/publication/14-02-13_letter_kessler_decision_en.pdf.

[37] [10] Available at https://edps.europa.eu/sites/default/files/publication/16-06-03_decision_data_transfer_ecb_en.pdf.

[38] [9] Available at https://edps.europa.eu/sites/default/files/publication/18-01-17_annex_2017-1120_en.pdf.

[39] [8] Available at https://edps.europa.eu/sites/default/files/publication/19-03-13_edps_decision_concerning_iosco-esma_administrative_arrangement_en.pdf.

(2) the transfer is occasional and necessary for the *performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request*;

(3) the transfer is occasional and necessary for the *conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person*;

(4) the transfer is necessary for *important reasons of public interest* recognised in Union law such as international data exchange between Union institutions and bodies and competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of *contact tracing for contagious diseases* or in order to reduce and/or eliminate doping in sport (Recital 69 of the Regulation);

(5) the transfer is occasional and necessary for the establishment, exercise or defence of *legal claims*, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies (Recital 68 of the Regulation);

(6) the transfer is necessary to protect the *vital interests* of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(7) the transfer is made from a *register* which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest,[40] but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case. This transfer must not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by Union law. Where the register is intended for consultation by persons having a legitimate interest, the transfer must be made only at the request of those persons or if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject (Art. 50(4) and Recital 68 of the Regulation).

Transfers based on the derogation for the specific situation of contact tracing (Recital 69 and Art. 50(1)(d) of the Regulation) are especially relevant to the COVID-19 pandemic. Last, Art. 50(6) of the Regulation provides that Union institutions and bodies must notify the EDPS about the categories of cases in which this provision has been applied.

[40] Art. 50(1)(g) of the Regulation provides for the notion of "legitimate interest" as the applicable test for access by a person to the register for consultation. Article 5 of the Regulation on lawfulness of processing does however not set out legitimate interest as a legal basis for Union institutions and bodies to process personal data. Conversely, Art. 6(1)(f) of the GDPR provides that legitimate interests are one of the six legal bases for controllers or third parties to process personal data.

5 Conclusion

Analysis of Chapter V of the Regulation shows that the general principles, the approach, the architecture and the legal bases which apply to transfers of personal data by Union institutions and bodies to third states and international organisations are unsurprisingly consistent with those which are provided for in both the GDPR and the Law Enforcement Directive to which Chapter V of the Regulation abundantly cross-refers. The legal bases set out in Chapter V of the Regulation are simply tailor-made to the specific needs of Union institutions and bodies. Recital 69 and Art. 50(1)(d) of the Regulation on the derogation for the specific situation of contact tracing provide a useful legal basis in the context of the COVID-19 pandemic, thereby showing that Chapter V of the Regulation includes appropriate tools to tackle the challenges of our times.

The *Schrems* II judgment is legally based *inter alia* on Article 7 about the respect for private life, Article 8 about the protection of personal data and Article 47 about the right to an effective remedy of the Charter. The latter which is part of EU primary law applies to Union institutions and bodies, pursuant to Art. 51(1) of the Charter. The *Schrems* II judgment has therefore far-reaching implications for Union institutions and bodies. The EDPS assists and supports Union institutions and bodies in properly dealing with such implications.

Last but not least, the extremely limited number of adequacy decisions issued by the Commission shows the increasing practical importance of appropriate safeguards as a legal basis to transfer personal data by Union institutions and bodies to third states and international organisations. In this respect, Union institutions and bodies are in a similar situation as all controllers in both the GDPR and the Law Enforcement Directive. In this context, the availability of updated standard contractual clauses is a welcome development.

References

1. Authorisation decisions of the European Data Protection Supervisor for transfers of personal data pursuant to Article 9(7) of Regulation 45/2001. Available at https://edps.europa.eu/data-protection/our-work/our-work-by-type/authorisation-decisions-transfers_en
2. C-311/18 *Facebook Ireland and Schrems*, EU:C:2020:559
3. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76/1
4. Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [2021] OJ L 199/31
5. Commission Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en
6. Commission Implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final. Available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en

7. Decision of the European Data Protection Supervisor dated 13 February 2014 on transfers carried out by OLAF through the Investigative Data Consultation Platform. Available at https://edps.europa.eu/sites/default/files/publication/14-02-13_letter_kessler_decision_en.pdf
8. Decision of the European Data Protection Supervisor dated 13 March 2019 on the use of the Administrative Arrangement by the European Securities and Markets Authority. Available at https://edps.europa.eu/sites/default/files/publication/19-03-13_edps_decision_concerning_iosco-esma_administrative_arrangement_en.pdf
9. Decision of the European Data Protection Supervisor dated 17 January 2018 on transfers by the European Centre for Disease Prevention and Control to the World Health Organization. Available at https://edps.europa.eu/sites/default/files/publication/18-01-17_annex_2017-1120_en.pdf
10. Decision of the European Data Protection Supervisor dated 3 June 2016 on transfers by the European Central Bank for its supervisory activities. Available at https://edps.europa.eu/sites/default/files/publication/16-06-03_decision_data_transfer_ecb_en.pdf
11. 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, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89
12. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
13. Draft adequacy decision of the Commission about the UK on the basis of the GDPR. Available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf
14. Draft adequacy decision of the Commission about the UK on the basis of the Law Enforcement Directive. Available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf
15. Draft implementing decision on standard contractual clauses for transfers of personal data to third states proposed by the Commission, pursuant to Article 46(2)(c) of the GDPR. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
16. EDPB Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020
17. EDPS Decision authorising, subject to conditions, the use of the administrative arrangement between the European Commission and the Turkish Medicines and Medical Devices Agency in the context of the Turkish participation in the EU regulatory system for medical devices Eudamed (Case 2021-0347), 12 May 2021. Available at https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/edps-decision-authorising_en
18. Joint opinion 2/2021 of the European Data Protection Board and the European Data Protection Supervisor dated 14 January 20221 on draft standard contractual clauses for transfers. Available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en
19. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom. 13 April 2021. Available at https://edpb.europa.eu/our-work-tools/our-documents/other/opinion-152021-regarding-european-commission-draft-implementing_en
20. Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. 13 April 2021. Available at https://edpb.europa.eu/our-work-tools/our-documents/other/opinion-142021-regarding-european-commission-draft-implementing_en
21. Press release EDPS/2021/11 of 27 May 2021, The EDPS opens two investigations following the 'Schrems II' Judgement. Available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en
22. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, 9.12.2020, COM(2020) 796 final, 2020/0349 (COD)

23. Recommendations 01/2021 of the European Data Protection Board dated 2 February 2021 on the adequacy referential under the Law Enforcement Directive. Available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en
24. Recommendations 02/2020 of the European Data Protection Board dated 10 November 2020 on the European Essential Guarantees for surveillance measures. Available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en
25. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1
26. Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/89
27. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39
28. Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA [2018] OJ L 295/138
29. Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1
30. Resolution of Parliament dated 21 May 2021 on the adequate protection of personal data by the United Kingdom. Available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html
31. Strategy dated 29 October 2020 of the European Data Protection Supervisor for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling. Available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf
32. Tracol, X.: 'Invalidator' strikes back: The harbour has never been safe. Comput. Law Secur. Rev. **32**(2), 345–362 (2016)
33. Tracol, X.: The two judgments of the European Court of Justice in the four cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention. Comput. Law Secur. Rev. **41**, 12–13 (2021)
34. Tracol, X.: Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada. Comput. Law Secur. Rev. **34**(4), 840–842 (2018)
35. Tracol, X.: Schrems II: the return of the Privacy Shield. Comput. Law Secur. Rev. **39**, 1–11 (2020)
36. Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L 149/10