UiT The Arctic University of Norway

Faculty of Law

Third country transfers of personal data under the GDPR: A review on remote access to personal data for business purposes

In the light of C-311/18 *Schrems II* and new practices from the European Data Protection Board

Victoria Helen Jakobsen

Master's thesis In Master of Law, JUR-3902, May 2022

Table of Contents

1 Introduction

1.1 Background

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("The GDPR") repealed and replaced the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("The DPD") in 2016.

On 25 May 2018[1], two years after its enactment, "the most contested law in the EU's history" became enforceable[2].

The EU and the European Economic Area ("EEA") has with the GDPR managed to influence tens of other national or regional jurisdictions who have developed their privacy and internet laws very much following the essence and cornerstone elements of European legislation[3]. The EU trades in digital services with the US is $260 billion worth annually, much of which involves personal data[4]. The economic aspects, combined with the data protection irregularity between countries, clarify much of the global interest in the GDPR[5].

More people are connected online, and even more businesses are relying on remote access to data for their employees to seamlessly access their workspace from home or beyond boarders. This thesis will illustrate the legal landscape for the cases of remote access to personal data in business-to-business relations under the GDPR considering new case law and practices.

Recital 6 to the GDPR underlines rapid technological developments and globalisation as causes for new challenges for the protection of personal data. Recital 6 further states that both "the scale for collection and sharing of personal data has increased significantly", which again allows public authorities and private companies to "make use of personal data on an

---

[1] See article 99 of the GDPR.

[2] Powles, J. (2018)

[3] Greenleaf (2012.)

[4] Schwartz and Peifer (2017) pages 106, 115–179.

[5] Georgiadou, de By, Kounadi (2019), page 157.

unprecedented scale". The GDPR is therefore a comprehensive regulation that creates a framework for the collection, processing, storage, and transfer of "personal data".

Art. 4 (1) of the GDPR offers the definition of "personal data" to mean any "information relating to an identified or identifiable natural person".

A data subject is then defined in the same provision as an identifiable natural person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". As understood of the phrasing in article 4 (1), the scope of "personal data" has a wide coverage.

1.2 Issue of the thesis

1.2.1 An introduction to transfer tools under the GDPR

GDPR Chapter V requires that any transfer of personal data from the EU/EEA to a third country[6] is subject to restrictions, so to ensure that the level of protection is not undermined, see art. 44 and the developments of the case C-311/18 *Schrems II* [7].

The imperative wording of article 44 of the GDPR is that "the level of protection" is not "undermined". Chapter 3 of this thesis will assess exactly what level of protection article 44 and The *Schrems II* case refer to.

Article 45 and 46 of the GDPR sets out the different transfer tools to base a transfer of personal data on. In other words, a transfer tool is a necessary instrument to legally transfer personal data. Article 49(5) does however set out derogations allowing transfer of personal data without such transfer tools in place, these derogations will not be discussed further in this thesis.

[6] Or an international organization. This will however not be the focus of this thesis.

[7] This is further supported in the Recital 101 where it states that "when personal data are transferred from the union to(...)recipients in third countries(...)the level of protection(...)ensured in the union by this regulation should not be undermined(...)".

Article 45 of the GDPR describes the adequacy decision, which is where the "Commission has decided that the third country (…) ensures an adequate level of protection".

In the Case of *Schrems II*, the Court of Justice of the European Union ("CJEU" or "the Court") addressed the claim that Facebook Ireland could not transfer the information about Maximilian Schrems to Facebook Inc. located in the US. The Court annulled the adequacy decision "Privacy Shield" between the Union and the US on the basis that the Privacy Shield did not provide an adequate level of protection after all.

As of 25th of March 2022, the Commission and the US has reached a Trans-Atlantic data privacy framework to replace the invalid Privacy shield[8]. This must not be confused with an adequacy decision. At this point, this announcement does not constitute a legal framework on which companies can base their data transfers to the United States. Companies wishing to transfer personal data to the US, must therefore continue taking the actions required to comply with the case law of *Schrems II* [9]. Adequacy decisions and the *Schrems II* judgement on the invalidation of Privacy Shield will be elaborated on in Chapter 4.2 of this thesis.

The lack of an adequacy decision gives rise to what other transfer tools one can use when transferring personal data to third countries without undermining the protection of personal data. Article 46 (1) details that "appropriate safeguards" may be that of, *inter alia*, Standard Data Protection Clauses adopted by the European Commission, Binding Corporate Rules, or Codes of Conduct. This thesis will focus on Standard Data protection Clauses and Binding Corporate Rules, see Chapter 4.3, 4.4 and 4.5 of this thesis.

As will be seen in Chapter 4.6, if the situation in the third country requires it, a data importer[10] or a data exporter[11] may still need to complement their transfer tools with "additional safeguards" to provide an adequate level of protection[12].

---

[8] See Chapter 4.2.2. of this thesis and C-311/18 *Schrems II.* See also the EDPB Statement (01/2022) page 1.

[9] EDPB Statement (01/2022) page 1.

[10] The receiving party of the data transfer, often in a third country.

[11] The party sending data out of the EU/EEA

[12] See also Chapter 3.1 of this thesis.

1.2.2 An introduction to remote access to data

Because of the *Schrems II* judgement, the European Data Protection Board ("The EDPB") adopted the Recommendations on measures that supplement transfer tools to ensure compliance with the EU/EEA level of protection of personal data ("The EDPB Recommendation (01/2020)"). This thesis will build upon the use case 7 of this Recommendation[13].

The case outlines the event that a data exporter transfers personal data to an entity in a third country for shared business purposes either by electronic transmission or by making it available through remote access by the data importer.

Electronic transmission could, *inter alia,* be by means of e-mail services. Whereas remote access to data would be the case where a data exporter in the EU/EEA gives access to data stored in the EU/EEA to a data importer in a third country. In other words, the data itself has not been transmitted, but the data is nevertheless *available* from a third country.

An example of remote access to data could be when a company in Denmark gives access to a server in the EU storing the personal data of its employees to the parent company in the US. This could be because the US parent company needs the data to provide personnel services or to satisfy rules and practices in US company legislation.

Another example of remote access could be that a Norwegian company uses a cloud service provider to organize or complete tasks important for the company. This could be the use of an online storage of files containing personal data on clients or business partners. The cloud service provider is then storing the files in a third country with remote access given to the Norwegian company.

In these cases, it's important to note that it's not, in itself, unlawful to use a cloud service provider who's established in a third country[14]. The service provider could, for instance, operate though an EU/EEA subsidiary with servers in Union territory. Consequently, there would be no access of data from outside the EU/EEA.

[13] The EDBP Recommendation (01/2020) page 35

[14] Danish DPA Guidelines (03/2022)page 28.

The problem of this thesis arises where the third country parent company or cloud service provider receives *access* to the data stored on the European servers[15]. Such disclosure could interfere with the standards of data protection in the Union, e.g. In situations of surveillance from state authorities in the third country[16]. In these situations, it is presumably the *access* from a third country parental company or cloud service provider that require transfer tools and safeguards as set forth in Chapter V of the GDPR and subsequent caselaw from the CJEU[17]. This will be further elaborated on in Chapter 2 of this thesis.

The EDPB uses the terms "data importer" and "data exporter", these terms give an understanding of who is sending and receiving the personal data that is being transferred, but the terms are not found in the GDPR. The Regulation uses the terms "controller" and "processor". Article 4 (7) defines "controller" as the "natural or legal person(…)or other body which, alone or jointly with others determines the purposes and means of the processing of personal data". The term "processor" is defined in art. 4 (8) as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

For this thesis, both the data importer and the data exporter may be a controller or a processor – this depends on the internal organisation of responsibility between the data importer and the data exporter. This thesis will therefore use the term "data importer" and "data exporter" when the internal organization is irrelevant, and the term "controller" and "processor" to indicate the internal organization of rights and responsibilities under the GDPR.

1.3 Method of EU law

1.3.1 The legal sources for this thesis

For this thesis, the relevant legislation is the GDPR, which is a regulation applying to EU and EEA Member States.

One of the main differences in the GDPR and the previous DPD is its legal form. A directive like the DPD, is binding, as to the result to be achieved, but shall leave to the national

---

[15] Danish DPA Guidelines (03/2022)page 28.

[16] See the case C-311/18 *Schrems II* and Chapter 4.2.2. and 4.4.2 of this thesis.

[17] See Chapter 2.4 and Chapter 4 of this thesis.

authorities of the Member States the choice of form and method[18]. The GDPR is a regulation and has general application in the Union. It is binding in its entirety and directly applicable in all Member States[19]. This ensures that European personal data is subject to harmonised rules throughout the Union.

A challenge in this thesis is that the GDPR is relatively new. Seeing that the regulation is a continuation of the previous DPD, decisions from the CJEU and other legal sources under the DPD can have relevance to the interpretation of the GDPR. However, it´s important to note that a legal examination applying older sources to the GDPR might not consider the current view of the legislators. When relevant, this will be addressed in the thesis[20].

Norway has incorporated the regulation as national law through the "Personal Data Act" in 2018[21]. Paragraph 2 (4) of the Personal Data Act states that the obligations under international or European law shall be favoured before Norwegian law where there is conflict between them. This method is to ensure legal conformity and means that the GDPR practically applies as the original version[22]. Therefore, the focus of this thesis will be on the legal sources on a European level, as this is binding on a national level as well[23].

The GDPR comprises of 99 provisions and 174 recitals in the preamble. The provisions are legally binding and the primary source. The method of the CJEU has been commented on by Advocate General Fennelly, it was noted that the characteristic element in the Courts interpretive method is the "teleological approach"[24]. The Court has given priority to the teleological method of interpretation over others because the Treaties are imbued with a

[18] Consolidated version of the Treaty on the Functioning of the European Union ("TFEU") art. 288 (3)

[19] See TFEU art. 288 (2)

[20] E.g., Chapter 2.2.2 of this thesis.

[21] The Personal Data Act (2018) Article1, with exceptions following by Attachment XI, protocol 1 and the Regulation as such.

[22] See Skoghøy (2018) page 128 and 131

[23] With some exceptions, see the GDPR article 6(2) where the regulation allows each member to give more specific provisions in national legislation.

[24] Lenaerts and Gutierrez-Fons, (2014), page. 31

purpose-driven functionalism[25]. Because of the Court´s teleological methods of interpretation it is not uncommon that the Recitals has an essential role in the interpretation of provisions.

The CJEU has previously stated in the case C-134/08 *Tyson Parketthandel* paragraph 16, that the preamble to a Union act has "no binding legal force and cannot be validly relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording…" Nevertheless, the Recitals contribute with clarification and understanding to the purpose of the provisions.

The Advocate General's duty is "to make, in open court, reasoned submissions on cases which (...) require his involvement" in order to "assist the (...) Court in the performance of its task"[26]. These submissions, which are known as AG opinions or just opinions, might play a role in the outcome of the cases before the Court. However, AG opinions are not binding on the CJEU, and the Advocates General do not take part in the Court's secrete deliberation[27]. As for the opinions legal value, it goes only as far as the opinions provide conviction, unless the CJEU offers its agreement in its judgement.

This thesis will also cite the European Data Protection Board Guidelines and Recommendations. On 25 May 2018 the EDPB formally replaced the Article 29 Working Party ("WP29") as the European advisory committee on data protection issues. The EDPB is established by the GDPR in article 68. The EDPB is an independent European body[28], that ensure the consistent application of the GDPR[29] and promotes cooperation between the EU's data protection authorities[30].

Amongst other tasks, The EDPB issue Guidelines, Recommendations, and best practices[31]. Recommendations and Opinions have no binding force under Union law, see TFEU article 288(5). Nevertheless, Guidelines and Recommendations of the EDPB reflect the common position and understanding which the authorities agree to apply in a consistent way.

---

[25] Lenaerts and Gutierrez-Fons, (2014), page. 31.

[26] Art. 252 TFEU and art. 49 of the CJEU statute.

[27] Arrebola, Mauricio & Portilla (2016) page 5

[28] See recital 139 of the GDPR

[29] see article 70(1) of the GDPR

[30] see article 62(7) of the GDPR

[31] *Inter alia,* article 70(1)(d)(e)(f)(g)(h)(j) and (m); For other tasks, see Recital 136 of the GDPR.

Therefore, they are an important source for understanding and interpreting the articles of the GDPR.

In the context of Norwegian law, the importance of EDPB Recommendations and Guidelines could be doubted. However, the purpose of harmonization and conformity implies that the Norwegian data protection authorities, when assessing a case, would consider the legal understanding and interpretation of the EDPB and other Member State authorities on the GDPR.

Another source used in this thesis is feedback from commercial and state actors to the EDPB recommendations and guidelines. These have no legal value beside their own power of conviction. Yet, they prove as a brief illustration of the opinions from the actors within the field of GDPR.

1.3.2 The application of the Charter and the ECHR

In the case of C-311/18 *Schrems II,* the referring court asked whether to assess the level of data protection within the EU/EEA in the light of the Charter of Fundamental Rights of the European Union ("The Charter"), or the European Convention for the Protection of Human Rights and Fundamental Freedoms ("The ECHR").

Article 6(3) of The Treaty on European Union ("TEU") confirms that the fundamental rights enshrined in the ECHR does constitute general principles of EU law. Furthermore, article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Nonetheless, the latter does not constitute a legal instrument which has been formally incorporated into EU law[32]. For the rights relevant to privacy and data protection, guaranteed in Articles 7, 8 and 47 of the Charter, they correspond to those enshrined in Articles 8 and 13 of the ECHR, and they share their meaning and scope.

However, EU law may afford them wider protection. The Attorney General emphasizes that the standards given in Articles 7, 8 and 47 of the Charter, as interpreted by the CJEU, are in

[32] C-311/18 *Schrems II* AG opinion paragraph 251

some respects stricter than those arising under Article 8 of the ECHR according to the interpretation by the European Court of Human Rights[33].

In *Schrems II*, there is a discrepancy between the Court and the Attorney General opinion; While the Attorney General, on the one hand, has a more open approach suggesting the best protection principle[34]. The Court, on the other hand, apply a more rigid interpretation based on case law, thus excluding the ECHR and only interpret the provisions in the light of the Charter[35]. The Court also emphasizes that that the interpretation cannot be construed in the light of national law, even national law of constitutional status, see C-11/70 *Internationale Handelsgesellschaft* paragraph 3[36].

Consequently, where relevant in this thesis, the provisions in the GDPR will be read in the light of the Charter and not the ECHR.

It would go too far for this thesis to assess and compare the material implications of the Charter on the field of data privacy. This could however be an interesting subject for further research.

2 The scope of the GDPR in the cases of remote access to data

2.1 The Concept of "processing" under the GDPR

The first question is whether remote access to personal data could constitute a processing as described under article 2 of the GDPR. This will determine whether the act of remote access falls within the material scope of the GDPR.

The criterion in article 2(2) is that the processing in question must be "wholly or partly by automatic means". The natural understanding of the phrasing, suggest that the process

[33] C-311/18 *Schrems II* AG opinion paragraph 251

[34] C-311/18 *Schrems II* AG opinion paragraph 249-253

[35] C-311/18 *Schrems II* paragraph 99-101

[36] C-311/18 *Schrems II* paragraph 100

contains an aspect of technology. This criterion is not problematic for this thesis as remote access to data would require the necessary technology to accomplish access in the first place.

The more problematic aspect of article 2 (1) is whether remote access is "processing of personal data".

The term "processing" is defined in art. 4 (2) of the GDPR to be any operation which is performed on personal data, "such as collection, recording, organisation, (…)disclosure by transmission, (…) or otherwise making available" data.

It's worth noting that the phrasing "such as" could imply that the article is not giving an exhaustive list, but merely examples of processing activities.

As seen above, the term "remote access" is not explicitly used. However, article 2 (1) use "disclosure by transmission". A natural understanding of "disclosure" would be a revelation or exposure of personal data to another party. To remotely access data, the data importer relies on a *disclosure* by a data exporter, even if it's not "by transmission" as the wording of article 2 (1) states. A teleological interpretation could suggest that remote access is covered by the term disclosure.

To further support this statement the article also covers "otherwise making available" data to another. To make something available would encompass a presentation of personal data to another party, who previously did not have access to the data. Which after its natural understanding would include a data importer remotely be given access to personal data.

In the case C-101/01 *Lindqvist*, Mrs. Lindqvist worked as a catechist in a parish in Sweden. Mrs. Lindqvist had set up internet pages on her computer to allow parishioners preparing for their confirmation to obtain any information they needed. She requested the administrator of the Swedish Church's website to set up a link between those pages and the website. The pages she had set up contained information about Mrs. Lindqvist and 18 of her colleagues in the parish.

The Court states in paragraph 25, that the operation of loading personal data on an internet page must be a processing covered by the DPD. This could further allow for an analogy that the uploading of personal data to a server with remote access should be considered a processing under the GDPR art. 2(1) and article 4 (2).

In the case C-362/14 *Schrems I,* Mr. Schrems argued the adequacy decision "Safe harbour" between the EU and the US was invalid. The Court then states that the operation of transferring personal data from Member State to a third country, constitutes in itself, processing of personal data within the meaning of article 4(2) of the GDPR[37].

Further supporting the fact that a remote access to data is in fact a "processing" under article 4 (2) and that the GDPR is applicable on these cases.

2.2 Remote access as a "transfer" under the GDPR

2.2.1 Introduction

Article 44 of the GDPR starts by indicating that a "transfer" of personal data is the elementary criteria for the following articles of Chapter V to come into effect. If the operation of remote access to data is not a "transfer of personal data", then there will be no need to implement transfer tools as Chapter V requires.

There is no explicit definition of transfer in the GDPR. Though, the European Data Protection Supervisor ("EDPS") and The European Parliament`s Committee on Civil Liberties, Justice and Home Affairs did call on the Union legislature to include a definition of "transfer" in the Privacy Regulation[38].

Article 44(1) states that "any transfer of personal data which are undergoing processing (…) after transfer to a third country (…) shall take place only if (…) the conditions laid down in this Chapter are complied with".

The phrase "after transfer *to a third country* (…)" (my cursives) could after a natural understanding advocate for a geographical allocation of data.

Recital 101 further confirms a geographical oriented understanding when stating "when personal data are transferred *from the Union to* (…) *recipients in third countries*(…)"(my cursives).

[37] C-362/14 *Schrems I,* paragraph 45

[38] EDPS Opinion (2012), page. 17 and COM (2012) 0011 page 65

However, a technological context could support a broader interpretation. Even if the data stays in the same European server, access to personal data from a third country could make the data accessible and disclosed to a broader group of natural or legal persons. And thus, suggesting that an access from a third country should be considered a "transfer" and invoke Chapter V of the GDPR.

Moreover, as underlined in Recital 101, the aim of Chapter V is to not undermine the level of protection of natural persons in the Union when data is in a third country. An undermining of the protection given in the EU could be just as possible in the context of remote access to personal data as when the data has been transmitted from the Union to the third country through *inter alia*, e-mail services. To ensure this goal, the cases of remote access should constitute a "transfer" in the understanding of art. 44(1). This understanding could, theoretically, find support in the CJEU given their teleological approach of interpretation, see Chapter 1.3 of this thesis.

2.2.2 C-101/01 *Lindqvist*

In the case of *Lindqvist*, it was a question whether uploading of personal data onto an internet page constituted a "transfer" of those data to a third country within the meaning of article 25 of the previous DPD. The reason being that such an upload would make the data accessible to people in a third country. In this case the CJEU concludes that the uploading was not a transfer within article 25 of the DPD. The weight of the case could be disputed because of its age and its relation to the DPD and not the currently effective GDPR.

The CJEU gave three predominant reasons for its conclusion, which I will assess below.

The Courts first reason is based on the procedures for use of the internet in the case of Mrs. Lindqvist, stating that these support the fact that an uploading is not a "transfer"[39]. The Court emphasized that it was necessary to take account "both the technical nature of the operations thus carried out"[40].

Especially, the Court seems to rely upon the fact that an internet user would have to connect to the internet and personally carry out the necessary actions to consult those pages. The

[39] C-101/01 *Lindqvist* paragraph 57-61

[40] C-101/01 *Lindqvist* paragraph 57

Court further states that the "internet pages did not contain the *technical means to send that information automatically to people who did not intentionally seek access to those pages*"(my cursives) [41].

In other words, there is a technological discrepancy between sending data and making them accessible. It could be noted that a cloud based filesharing system or other means of remote access solutions, could have the "technical means to send information automatically to people". Perhaps suggesting that the Courts first reason, is not applicable in these situations.

This justification has also been criticised for relying too much on whether the data were actually accessed. Christopher Kuner argues that this seems irrelevant and has been largely rejected by the EU data protection authorities in their interpretation of the case[42]. The key question should have been whether the data *could* have been accessed from a third country[43].

Should this understanding take precedence, the entire Chapter V of the GDPR would only be subject to direct transmissions, which seems to contradict the purpose of transborder protection of data as its anchored in Recital 101 to the GDPR.

As highlighted by Recital 6 to the GDPR, both the scale of the collection and sharing of personal data has increased significantly throughout the years. Technology now allows both private companies and public authorities to make use of personal data on an "unprecedented scale" in order to pursue their activities. As the technology has changed rapidly and innovatively since the early 2000, perhaps the Courts first reasoning did not withstand the test of time.

The Courts second reasoning in the case of *Lindqvist* was whether the legislature intended for the situations of access, and not direct transfers, to fall within the scope of Chapter IV of the DPD[44]. The Court built their argumentation around whether the DPD contained any provision relating specifically to the use of the internet, concluding that it did not[45]. Where they instead

---

[41] C-101/01 *Lindqvist* paragraph 60

[42] See Chapter 2.4 of this thesis

[43] Kuner (2013) page 13.

[44] C-101/01 *Lindqvist* paragraph 62

[45] C-101/01 *Lindqvist* paragraph 63-68

could have emphasized that the directive is technology neutral and thus should be applied independently of the technological methods[46].

Finally, the Court reasons around the international implication of its decision, stating that if the Court concluded otherwise the entire internet would be subject to European data protection law[47]. If the CJEU had concluded otherwise in this case, it would make for a radical expanding of the scope of the DPD.

Following the changes in article 3 of the GDPR in comparison to article 4 of the DPD, the GDPR has expanded the territorial scope of European privacy legislation. The application of the GDPR is, under certain conditions, independent of the place where processing of personal data takes place. The focus is the data subject and not the location. While the DPD made application of national law, a criterion for determining the applicability of the Directive[48]. This might suggest that the third reasoning of the Court is not as relevant under the GDPR as it was under the DPD.

Additionally, the DPD was a directive and not a regulation, thus giving the Member States freedom of incorporating the directive how they best saw fit. One could argue that such a wide scope for a directive would cause disharmony, even if it was harmony the EU legislature intended. It is possible that the CJEU saw the implication of its decision and decided that the disharmony of making the entire internet fall under the scope of the DPD was not a suitable outcome. If this indeed is the reasoning, the GDPR is much more fitted for such a wide scope, with a higher level of harmony required by the Member States and more derogations than its predecessor.

In the case of *Lindqvist*, it was clear that Mrs. Lindqvist herself had no intention of making the personal data available in a third country. Though the CJEU did not use this argument in its judgement, it's interesting to imagine whether the outcome would have been different if the case concerned commercial actors instead of a catechist from Sweden.

---

[46] Svantesson *Privacy, internet and Transborder Data Flows,* page 15

[47] Kuner *(*2013) and *Lindqvist* paragraph 69.

[48] See the DPD article 4.

2.2.3 Summary

The Court considers uploading on the internet, where access from a third country is possible, as not a "transfer" under the DPD. The Court gave three justifications, all of which has debatable value under the GDPR. The conclusion of the Court has also been ignored by the EDPB in its Guidelines 05/2021. Consequently, questioning the definition of transfer further.

Though the concept of "transfer" is not clear, the *Lindqvist* case cannot give precedence that remote access is indeed not a transfer under the GDPR.

2.3 The EDPB Guidelines on the concept of transfer

2.3.1 Availability as a criterion for transfer

To answer the question of whether remote access to data is a "transfer" under the GDPR Chapter V, there are not many other legal sources to rely on. However, since the *Lindqvist* case in the early 2000, the EDPB has released Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR ("EDPB Guidelines (05/2021)".

The EDPB has identified the tree following cumulative criteria that qualify a processing as a "transfer" [49].

First, a controller or a processor is subject to the GDPR for the given processing. Secondly, the data exporter discloses by transmission or *"otherwise makes personal data* (…) *available to the data importer"* [50] (my cursives). Finally, the data importer is in a third country, irrespective of whether this importer is subject to the GDPR.

A natural understanding of "available" supports an understanding that the content of something is presented to another, or that the content is offered and accessible to another. One could argue that there is a difference in presenting and accessing something. Presenting would

[49] The EDPB Guidelines (05/2021) page 4

[50] The EDPB Guidelines (05/2021) page 4

possibly constitute a show and tell of the content, while access – at least to some extent – require a sort of tangible possession of the content[51].

The European Data Protection Supervisory ("EDPS)" supports this understanding, stating that although there is no formal definition of "transfer", data exporters and data importers should consider that this term would normally imply *"disclosure or otherwise making available personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it"*[52].

Additionally, the Danish Data Protection Authority has released the "Guidance on the use of Cloud" of 03/2022. Specific for the use of cloud services is the ability to remotely access your files and platforms from the infrastructure of a cloud service provider. The Danish Data Protection Authority upholds that if a company intends to engage a cloud service provider located outside of the EU/EEA, the company must be aware of requirements when transferring personal data to third countries[53].

The aim of third country transfer restrictions is to not undermine the data protection given in the Union[54]. If personal data is *available* in third countries, this too could cause an undermining of the protection that was intended by the legislators, e.g., by surveillance from the third country state authority. Thus, supporting the conclusion that remote access, is a transfer in the context of Chapter V.

2.3.2 The relationship between a data controller and a data processor

The scope of the second criteria of the EDPB does except the situations where the data is disclosed from the data subject and to a data importer in a third country – this is because the exporting party is the data subject itself[55].

---

[51] The natural understanding of "available", combined with a technological point of view, does not exclude that there could be technical solutions, now or in the future, for remote access that could fall outside the scope of "transfer" by the EDPB. The determination of this would however require technological research not suitable for this thesis.

[52] EDPS (2014) page 7

[53] Danish DPA Guidelines (03/2022) page 17

[54] See Recital 101 of the GDPR

[55] See Sections 1–3 of the EDPB Guidelines (03/2018) And the EDPB Guidelines (05/2021) page. 4

The second criteria must therefore imply that to qualify as a "transfer", there must be a data exporter and a different data importer, each acting as a separate data controller or data processor.

This part of the thesis will illustrate the importance of these roles in the cases of remote access to data as a third country transfer. It would fall outside the scope of this thesis to assess the impact of company structures and international company law in too much dept.

As previously stated, the controller is the natural or legal person who, "determines the purposes and means of the processing of personal data", see GDPR art. 4(7). The data processor is the legal person "which processes personal data on behalf of the controller", see GDPR art. 4(8). The essential phrasing is "on behalf of the controller". A natural understanding suggests a business partner or a service provider to the controller.

The relationship between a data controller and a data processor is often given away by a data processing agreement between the parties[56]. As seen in Chapter 2.1 of this thesis, the definition of "processing" in article 4(2) of the GDPR is not limited to the listed activities or operations. This could make it challenging for a data processor to recognise whether their activity or operations in relations to a business partner actually constitutes a process and requires a data processing agreement.

Based on the phrasing of article 4(7), it's not a "transfer" of data when the employee of a data controller in the EU travels to a third country and accesses the data from there. The employee does not determine the purposes and the means of processing like a controller – his employer – would. Additionally, the employee would not be solely responsible for the processing of the personal data he handles for his employer, thus he cannot be seen as a data processor.

A question that then arises is in which circumstances entities in the same corporate group qualifies as separate controllers or processors, and thus answering if an access of personal data between them actually constitutes a "transfer" in the context of Chapter V of the GDPR.

[56]"Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller", See article 28 (3) of the GDPR.

As an example, an Irish company A, which is a subsidiary of the US parent Company B, discloses personal data of its employees to parent Company B to be stored in a centralized HR database by the parent company in the US.

In this case the Irish Company A processes personal data in its capacity of employer and hence as a controller, while the parent company B is a processor because of the storage. This disclosure would need a data processing agreement and would qualify as a transfer to a third country within the meaning of Chapter V of the GDPR[57].

The fact that both companies are part of the same corporation is irrelevant, what is of importance is whether the data importer have a role as a data controller or a data processor in relation to the data exporter in the EU.

As an example, if a danish establishment has an international office in Egypt, and the employees in Egypt has access to the same digital system as the danish, this would not count as a transfer to a third country.

The essential is that the Danish establishment remains the controller, and the Egyptian office does not constitute a data controller or a data processor in the relation to the danish establishment[58]. This would also be applicable for the cases where an employee has office from abroad, as long as that employee does not constitute an independent data controller or data processor in relation to its employer[59].

If the Egyptian office was acting as an independent processor or controller, e.g., as a subsidiary of the Danish establishment, this access would be a transfer[60].

As seen in the abovementioned example, not every data flow may qualify as a transfer of personal data, even if the data is accessed or available in third countries.

These arrangements can still impair the protection of the personal data due to conflicting national laws or government access in e.g., Egypt[61]. The controller is nonetheless accountable

---

[57] The EDPB Guidelines (05/2021) page. 7, see also GDPR art. 28 (3).

[58] Danish DPA Guidelines (07/2021) page 10

[59] Danish DPA Guidelines (07/2021) page 11

[60] Danish DPA Guidelines (07/2021) page 10

[61] Danish DPA Guidelines (07/2021) page 10

for its processing activities regardless of where they take place and must comply with the GDPR[62]. Because of this obligation to implement technical and organisational measures, a controller may determine that extensive security measures are needed – or even that it would not be lawful – to conduct or proceed with a specific processing operation in a third country. This is despite there being no "transfer" between a controller and a processor. *Inter alia*, a controller may conclude that employees cannot bring their laptops, to certain third countries[63].

2.3.3 Summary

Remote access to personal data is by the EDPB considered as a "transfer" of personal data. By their definition a "transfer" in the understanding of GDPR Chapter V requires a data exporter to make personal data available to a data importer located in a country outside the EU; and the data importer is distinct from the data exporter as it is acts as a data controller or data processor in relation to the data exporter. This also applies for transfers to another company within the same corporate group.

However, if the data exporter is sending personal data to their employee, this is not a restricted transfer. One could argue that the EDPB seemingly narrows the definition of "transfer" by appointing a criterion that the transfer is made between two separate data controllers/data processors.

The data exporter should under any circumstance be aware of their responsibility and they are nonetheless accountable for its processing activities regardless of where they take place and must comply with the GDPR. With respect to the case of remote access in business-to-business relations, it is therefore imperative to assess whether the transfer in question is within the same controller or processor. Consequently, making it imperative that businesses know their transfers, their role and, know the role of the receiving or accessing party.

---

[62] *Inter alia,* art. 24 covering the responsibility of the controller, art. 32 about security of processing, art. 33 about notification of a personal data breach, and art. 35 covering the Data Protection Impact Assessment, as well as art. 48 about transfers or disclosures not authorized by Union law, etc.

[63] The EDPB Guidelines (05/2021) page. 7.

3 The protection required in third country transfers of personal data

3.1 Standard of "essential equivalence" in third country transfers

Before examining the transfer tools under the GDPR Chapter V, its necessary to grasp the intention behind and level of protection transfer tools are meant to give in third country data transfers.

Article 44 of the GDPR, opens Chapter V by announcing that "all the provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined". That the level of protection shall not be undermined indicate that the *de facto* protection should be *essentially equivalent* wherever the data is in the world. The phrasing of this article suggests that there is a comparative aspect to data transfers.

Recital 108 of the GDPR states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with art. 46 (1) must "compensate for the lack of data protection in a third country". The CJEU in *Schrems II* further emphasises that such compensation is to "ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union"[64].

The Advocate Generals opinion in the *Schrems II* case points out that such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country "are afforded a level of protection *essentially equivalent* to that which is guaranteed" within the Union after the GDPR read in light of the Charter[65] (my cursives).

[64] C-311/18 *Schrems II* paragraph 95

[65] C-311/18 *Schrems II* paragraph 96 and the AG opinion paragraph 115.

The verification of the level of protection ensured in a third country necessarily requires a comparison, on the one hand, between the rules and practices in that third country, and on the other hand, the standards of protection in force in the Union[66].

If, after a comparison, the assessor finds that the personal data in question would fall under the scope of substandard legislation in a third country, e.g., surveillance laws that exceeds what is necessary in a democratic society and not proportionate, then the personal data affected by this is not afforded protection *essentially equivalent* to that is guaranteed within the union after the GDPR read in the light of the Charter art. 7, 8 and 47[67].

3.2 National security as an exception under Union law

3.2.1 The case of C-311/18 *Schrems II*

In the *Schrems II* case, the referring court asked the CJEU to clarify on the comparison between rules and practices in a third country and in the Union.

Article 2(2)(a) of the GDPR states that the regulation does not apply to the processing of personal data during an activity which falls outside the scope of Union law. Article 4(2) of the TEU regards the competence conferred from Member States to the Union, stating that the "national security remains the sole responsibility of each member state". The natural understanding of this phrasing seems to leave little room for the CJEU and other EU institutions to interfere with legislation meant to safeguard Member States national security. This entails that processing of personal data justified in national security is the sole responsibility of each Member State and falls outside the scope of Union law, and ultimately also the scope of the GDPR. The referring court asked whether third countries is given the same exception of legislation safeguarding national security in the comparison of rules and legislation.

The case of *Schrems II* concerned US surveillance laws, FISA 702 and the basis for the PRISM and UPSTREAM surveillance programs. According to the PRISM programme, internet service providers are required to supply the NSA with all communications to and

[66] C-311/18 Schrems *II* AG opinion Paragraph 202

[67] See chapter 1.3.2 of this thesis.

from an individual of interest[68]. The UPSTREAM programme requires telecommunications undertakings operating the hardware of the internet – cables, switches, and routers – to allow the NSA to copy and filter internet traffic flows to acquire communications from, to or about a non-US national associated with an individual of interest[69]. The US Executive Order 12333 allows the NSA to access data "in transit" to the US by accessing underwater cables on the floor of the Atlantic. Thus, collecting and retaining such data before it arrives to the US, and before it can be subject to the FISA. It adds that activities conducted pursuant to the E.O. 12333 are not governed by statute[70].

All these legislations were justified in the safeguarding of national security in the US.

If a similar exception as article 2(2) of the GDPR and 4(2) of the TEU would be applicable when examining the rules and practices in third countries, the surveillance of the US authority done in the purpose of national security would be excepted. The utmost consequence of such an exception could be that the overall data protection in the US is *essentially equivalent* to that in the Union.

The Attorney General Opinion emphasizes in paragraph 204 that the *rasion d'être*[71] for the restrictions on international transfers of personal data, is designed to avoid the risk that the standards applicable within the Union will be circumvented. With national security as an exception and within the sole responsibility of each Member State, it is plausible that the standard within the Union and within each Member State entails similar legislation to that of the US. Thus, no standards would be circumvented or undermined. The Attorney General further states that "it would be wholly unjustified, having regard to that objective, if a third country were expected to comply with requirements that did not correspond to obligations borne by the Member States"[72].

The CJEU argues otherwise in their judgement of *Schrems II*. The Court initially states that it should be made clear that «the rule in Article 4(2) TEU (…) concerns Member States of the

---

[68] C-311/18 *Schrems II* paragraph 61.

[69] C-311/18 *Schrems II*, paragraph 62.

[70] C-311/18 *Schrems II*, paragraph 62.

[71] Reason or justification for existence.

[72] C-311/18 *Schrems II* AG opinion paragraph 204

European Union only». The Court finds this rule irrelevant for the purposes of interpreting Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR[73].

This statement does however not correspond with the purpose behind the standard of essential equivalence since the state of rules and practices in the Union could possibly be afflicted by such an exception. To state that this exception is irrelevant in third country transfers suggest that the standard of essential equivalence perhaps is not equal after all.

The CJEU further states in paragraph 85 that in this case, the transfer of personal data is between two legal persons – Facebook Ireland to Facebook Inc. – and consequently this transfer cannot fall outside the scope of the GDPR after article 2(2)[74]. This is despite that the problematic surveillance is done by US authorities which Facebook Inc. cannot control.

The Court relies particularly on the fact that the transfer is between two economic operators for commercial purposes. The possibility that such a transfer might undergo processing for the purposes of public security, defence, and State security, by the authorities of that third country cannot remove that transfer from the scope of the GDPR[75].

The CJEU further reasons that when the Commission is assessing the adequacy of the level of protection afforded by a third country, article 45(2)(a) of the GDPR states that they need to take account of "relevant legislation (…) including concerning public security, defence, national security". The Court states that it is self-evident from the very wording of Article 45(2)(a) that processing of personal data by a third country for the purposes of national security cannot exclude the transfer from the application of the GDPR[76].

This conclusion can cause a discrepancy in the standard of data protection the CJEU demands from third countries compared and the standard of data protection one might find in a Member State who uses the exception for national security under article 2(2)(a) of the GDPR read in the light of article 4(2) of the TEU.

---

[73] C-311/18 *Schrems II* paragraph 81

[74] See also Chapter 3.1.1.1. of this thesis.

[75] C-311/18 *Schrems II* paragraph 86

[76] C-311/18 *Schrems II* paragraph 87, 88 and 89.

The peculiar situation is therefore that the standard of essential equivalent protection is in fact not equivalent. Because of Member States legislation for safeguarding national security, the protection required from third countries might in some cases be higher than the *de facto* protection in Member States when assessing Union law as well as their national legislation.

3.2.2 Surveillance in the Union under the justification of national security

This section will demonstrate the surveillance situation in the EU/EEA and the room for exceptions under article 4(2) of the TEU. This is to clarify whether the exception for national security under the GDPR art. 2(2) and art. 4(2) TEU results in a higher *de facto* protection for personal data from third countries than in the Union.

It has been widespread practice among national security agencies in the EU/EEA to collect and access personal data in the field of electronic communications for safeguarding national security and combating crime. Four separate proceedings were brought against national legislations in United Kingdom, France and Belgium concerning the lawfulness of a general and indiscriminate retention obligation imposed on providers of electronic communication services.

One of these cases were C-623/17 *Privacy International*. The case concerned national legislation enabling a state authority to require providers of electronic communication services to forward traffic data and location data to the intelligence agencies for the purpose of safeguarding national security.

The first question of the referring court concerned the scope of Directive 2002/58 on privacy and electronic communications ("the E-privacy directive") after reading article 1(3) in the light of article 4(2) TEU[77].

After stating that art. 1(3) excludes the activities concerning public security, defence, and State security from the scope of the E-privacy directive. The CJEU then assess other articles of the E-privacy directive, even though they do not expressly concern the scope of application.

[77] C-623/17 *Privacy International* Paragraph 30

Article 15(1) expressly authorizes the Member States to adopt measures of public and state security only if specific conditions are met. Reliant on the wording of this article, the CJEU states that this article presumes that national legislative measures referred to therein fall within the scope of the E-privacy directive [78]. The Court then reasons that a derogation for national security after article 4(2) TEU would then deprive article 15(1) of any practical effect[79]. Thus, the Court concludes that an interpretation of article 1(3) of that directive in the light of article 4(2) of the TEU cannot be understood as covering the legislative measures referred to in article 15(1) of the E-privacy directive [80].

Though the Court agrees that it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, "the mere fact that a national measure has been taken for the purpose of protection national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law"[81].

This shows that even though there is a general exception in article 4(2) TEU, this does not include the situations where the Member States have given away competence in specific EU legislation. In other words, articles and rules in EU directives or regulations surpasses the general exception of article 4(2) TEU. This could be seen as an argumentation constructed from *Lex Specialis*[82].

Nevertheless, given the authority of the TEU compared to directives and regulations, the CJEU could have argued a *Lex Superior* in the defence of a general exception after article 4(2) TEU. The fact the CJEU would rather argue on *Lex Specialis* may be because of the teleological approach of the Court. A conclusion like this could possibly provide a higher level of harmonisation, as was envisioned by the E-privacy directive.

---

[78] C-623/17 *Privacy International* Paragraph 38

[79] C-623/17 *Privacy International* Paragraph 42

[80] C-623/17 *Privacy International* Paragraph 43

[81] C-623/17 *Privacy International* Paragraph 44

[82] Mæhle and Aarli (2017) page 330 and 331.

The CJEU then argues that their previous caselaw, C-317/04 and C-318/04 *Parliament v Council and Commission,* cannot hold precedence that will alter their conclusion in the case of *Privacy International*[83].

In these cases, the Court held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism fell outside the scope of article 3(2) of the DPD, because such a transfer fell within the framework established by the public authorities relating to national security[84]. One might note that the cases are from shortly after the terrorist attack of 9/11 in the US.

The Court points out that the conclusion in the previous case-law is reliant on the scope of the DPD and the phrasing therein. In the DPD there was no distinction on by whom the processing was done. Thus, excluding in a general way all processing operations concerning public security, without drawing any distinction according to who was carrying out the data processing operation concerned[85].

The CJEU then considers the scope of the GDPR because it has replaced the DPD[86]. The GDPR states in Article 2(2)(d) that it does not apply to processing operations carried out "by competent authorities" for the purposes of, *inter alia*, the safeguarding public security. The phrasing of the exception of article 2(2) (d) identifies that only operations carried out by competent authorities are to be excluded. The Court also finds support in Article 23(1)(d) and (h) of the GDPR that the processing of personal data carried out by individuals for those same purposes falls within the scope of the GDPR.

It follows that the understanding of the scope of the E-privacy directive is consistent with the understanding of scope of the GDPR[87]. It is also apparent that the CJEU reasons the same in

[83] C-623/17 *Privacy International* Paragraph 47

[84] C-623/17 *Privacy International* Paragraph 47

[85] C-623/17 *Privacy International* Paragraph 46

[86] Since the cases of C-317/04 and C-318/04 *Parliament v Council and Commission* the GDPR repealed and replaced the DPD.

[87] C-623/17 *Privacy International* paragraph 47

the case of *Privacy International* as it did in *Schrems II* regarding the scope of application and the derogation for national security[88].

When a directive expressly states by whom derogations for national security can be made – E.g., "by national authorities" – a national legislation imposed on economic operators will interfere with a directive because economic operators still are obliged to follow the rules and practices of the directive in question.

By contrast, where the Member states directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by the E-privacy directive or the GDPR, but by national law[89].

Consequently, meaning that even though there are limitations to the exception of article 4(2) TEU as interpreted by the CJEU in *Privacy International*, there is an exception for national security that third countries do not benefit from in the assessment of *essentially equivalent protection.*

3.2.3 Summary

This examination demonstrates that there are exceptions from directives and regulations anchored in article 4(2) of the TEU and thus the GDPR that are applicable for Member States. It also shows that these derogations from 4(2) of the TEU is not considered when assessing whether third countries provide *essentially equivalent protection*. Possibly requiring a higher protection from third countries than in Member States.

Even though the wording of article 4(2) of TEU is broad and without conditions, there are limitations. An exception for national security must be determined on a case-by-case basis, depending on the scope of the directive or regulation in question. The assessment of the scope is also done by assessing all the articles in the relevant EU legislation. Therefore, Member

[88] The assessment of by whom the processing operation is carried out, economic operator or a national security agency. Compare C-623/17 *Privacy International* paragraph 48 and C-311/18 *Schrems II* paragraph 86.

[89] C-623/17 *Privacy International* paragraph 48

States have given up more of their competence regarding national security than what is apparent from the very wording of article 4(2) TEU.

4 Transfer tools under the GDPR

4.1 Introduction

As seen in Chapter 1.2.1 there are several possible transfer tools available for a data exporter wishing to transfer personal data to a third country data importer. This Chapter will demonstrate the most common transfer tools of the GDPR; an adequacy decision, Standard Data Protection Clauses, and Binding Corporate Rules. In the end I will clarify some additional safeguards available for remote access to personal data transfers.

4.2 Adequacy decision

4.2.1 An introduction to the adequacy decision

A transfer of personal data may take place where the Commission has decided that the third country ensures an "adequate level of protection", see article 45(1) of the GDPR. The phrasing of art. 45(1) suggest that the level of protection needs to meet certain standards to be deemed "adequate". But the wording alone is otherwise silent on what those standards might be.

The concept of "adequate level of protection" in a third country must be *essentially equivalent* to that guaranteed in the EU/EEA[90]. The WP29 underlines that the objective is not to mirror point by point the European legislation, but to establish the essential requirements of that legislation[91].

Article 45 (2) of the GDPR, determines the elements that the Commission shall consider when assessing the adequacy of the level of protection in a third country. *Inter alia,* the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence, and effective functioning of one or

[90] See Chapter 3 of this thesis

[91] WP29 (2017) page 2

more independent supervisory authorities and the international commitments the third country has entered[92].

The underlying minimum requirements for data protection to be adequate are derived from the Charter of fundamental human rights and the GDPR, see Chapter 1.3.2 of this thesis.

The WP29 additionally clarifies that the concept of "adequate level of protection" under art. 45 of the GDPR includes two basic elements. First, the content of the rules applicable to the processing of data; Secondly the means for ensuring their effective application[93].

This entails that data can be lawfully transferred to third countries when the basic EU data protection principles continue to apply to the processing of data after transfer and when certain procedural and enforcement mechanisms are in place to ensure the effective implementation of those principles[94].

Under article 288 (4) TFEU, a Commission adequacy decision is, "in its entirety binding" on all the Member States to which it is addressed. After its natural understanding, its presumably also binding on all their organs, *inter alia* the national supervisory authority[95]. The effect of an adequacy decision is assimilating the third country transfer to intra-EU transfers of personal data. An adequacy decision will not need further authorization to be used, and therefore is a reliable way of exporting data out of the EU.

Article 46 (1) first sentence states that "in the absence of a decision pursuant to article 45 (3)" one may rely on the transfer tools in art. 46. This insinuates that the preferred transfer tool is an adequacy decision found in article 45.

The critics of this point of view, argues that there is no logical reason to assume that one transfer instrument may be proffered. None of them may adhere to lower standard than

---

[92] WP29 (2017) page 4

[93] WP29 (2017) page 3

[94] WP29 (2017) page 3

[95] C-362/14 *Schrems I* paragraph 51 and C-311/18 *Schrems II* paragraph 96 and the AG opinion paragraph 115. See Chapter 3.1. of this thesis.

another. None of them may "undermine" the standards of the GDPR, and all of them must provide *essentially equivalent protection*[96].

Recital 103 of the GDPR states that the Commission may decide with effect for the entire Union that a third country "offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the union as regards the third country". Hence, making an adequacy decision both predictable and beneficial. This could perhaps explain why an adequacy decision is presumably the preferred transfer tool for both the EU legislators and the data exporters and data importers.

Unfortunately, there are a limited number of third countries who have acquired an adequacy decision[97].

4.2.2 Invalidation of adequacy decisions

In the case of *Schrems II,* the referring court had doubts as to whether US law in fact ensured the adequate level of protection under article 45 of the GDPR read in the light of the fundamental right guaranteed under articles 7, 8 and 47 of the Charter.

Facebook Ireland formed their arguments based on article 288 of the TFEU, stating that an adequacy decision by the Commission is binding on all Member States. Facebook Ireland then claimed that the adequacy decision Privacy Shield was binding on the national supervisory authority, the Commissioner, and the CJEU itself.

However, the Court underlines that in any event, an adequacy decision adopted pursuant to article 45 (3) of the GDPR cannot prevent persons from lodging a complaint within the meaning of article 77(1) of the GDPR with the national supervisory authority.

Furthermore, an adequacy decision cannot eliminate or reduce the powers granted to the national supervisory authority by the Charter and article 51(1) and article 57(1) (a) of the

[96] Feedback NOYB (21.12.2020) page 2.

[97] The European Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.

GDPR. Meaning that if the enforcement of the GDPR requires it, a supervisory authority could adopt measures contrary to that decision, see article 57 (1) (a) of the GDPR[98].

Though, the supervisory authority cannot invalidate an adequacy decision itself. They must, nevertheless, be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring action before the national courts for them to make a reference for a preliminary ruling for the purpose of examining the validity of the adequacy decision in question[99].

The CJEU found that the Privacy Shield between the EU and the US didn't provide an adequate level of protection, thus turning the decision invalid.

4.2.3 Summary

In conclusion, a transfer of personal data based on an adequacy decision is a predictable and presumably preferred transfer tool, both by the data importer and data exporter, but also from the point of view of the EU legislators, see art. 46 (1) first sentence. Since there are few countries with an adequacy decision, it's not the most common transfer tool. A data exporter wishing to transfer data to a third country without an adequacy decision would need to make use of the appropriate safeguards in article 46[100].

For remote access to data, the *Schrems II* judgement came with imperative remarks and changes to the legal situation. First and foremost, by invalidating the adequacy decision Privacy Shield between EU and the U.S, making EU-US data transfers more complicated than it was under the Privacy Shield.

Schrems II also gives precedence that an adequacy decision is not absolute. The supervisory authority still has the powers granted to them under the GDPR, and the CJEU has the power to invalidate adequacy decision[101]. Perhaps also removing some of the predictability of an adequacy decision.

---

[98] C-311/18 *Schrems II* paragraph 119.

[99] C-311/18 *Schrems II* paragraph 120

[100] See Chapter 4.3 of this thesis

[101] C-311/18 *Schrems II* paragraph 157

This leaves it up to the data importer and the data exporter to be aware of their transfers and the national legislation of the third country in question.

4.3 Appropriate safeguards under the GDPR

In the absence of an adequacy decision, a data exporter may only transfer personal data to a third country if they provide "appropriate safeguards" and "on condition that enforceable data subjects rights" and "effective legal remedies for data subjects are available", see article 46(1) of the GDPR.

A natural understanding insinuates that there are three cumulative notions to legally transfer data under this article. First, there must be an appropriate safeguard, secondly that safeguard must provide the data subject with enforceable rights. Lastly, the data subjects must be afforded effective legal remedies.

What lies in the criteria of appropriate safeguard is further elaborated on in article 46(2). The last two conditions seem to complement the first notion by distinguish the most vital rights of the data subject. Seemingly, it's not enough to simply make use of one of the appropriate safeguards as mentioned in article 46(2) letter (a) to (f), if a data exporter cannot provide for enforceable data subject rights and effective legal remedies. Hence, emphasizing the necessity for *de facto* protection.

4.4 Standard Data Protection Clauses

4.4.1 An introduction to Standard Data Protection Clauses

An appropriate safeguard may be by making use of Standard Data Protection Clauses adopted by the Commission, see article 46(2) (c)[102]. The wording in article 46(2) (c) does not state what Standard Data Protection Clauses are or entail, just that one might make use of them. The Commission implemented new Standard Data Protection Clauses ("SCC (EU) 2021/914") in June 2021[103].

[102] Recital 108 first sentence.

[103] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

It would lead to far for this thesis to give a thorough assessment of the material content of the Standard Data Protection Clauses, but this Chapter will give an overview of their purpose and content.

Standard Data Protection Clauses are contractual obligations between data importers and data exporters to provide for data protection *essentially equivalent* to that of the Union, even if the laws and practices of a third country do not require it[104].

In Recital 19 to the SCC (EU) 2021/914, its stated that the transfer of personal data under Standard Data Protection Clauses "should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses". Implying that the Standard Data Protection Clauses must provide a binding effect and actual *de facto* protection.

Recital 19 further underlines that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society, should not be considered as conflicting with the standard contractual clauses. According to the assessment of Chapter 1.3.2 of this thesis, this could be seen as a reference to the fundamental rights and freedoms of the Charter.

Amongst others, Standard Data Protection Clauses require the data importer to notify the data exporter if the data importer has reason to believe that it is not able to comply with the Standard Data Protection Clauses, see Recital 21 of the SCC (EU) 2021/914. If the data exporter receives such notification or otherwise becomes aware that the data importer is no longer able to comply with the Standard Data Protection Clauses, it should identify appropriate measures to address the situation. If necessary, the data exporter should bring the matter to the competent supervisory authority. This makes Standard Data Protection Clauses less predictable than an adequacy decision and require more resources from the data importer and data exporter than an adequacy decision would.

The responsibility of investigating the laws and the practices of a third country falls upon the data exporter and the data importer. The parties should warrant that, at the time of agreeing to

[104] Hence why they often are called SCC as short for «standard contractual clauses».

the Standard Data Protection Clauses, they have no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements.

Recital 109 of the GDPR states that "the possibility for the controller or processor to use standard data-protection clauses adopted (...) should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract (…) nor from adding other clauses or additional safeguards". Implying that Standard Data Protection Clauses are not absolute and could be supplemented. Recital 109 further underlines that controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement Standard Data Protection Clauses.

4.4.2 The case of C-311/18 *Schrems II*

In the case of *Schrems II,* the CJEU starts by stating that "appropriate safeguards" is covered by the phrasing and understanding of article 44 (1). Concluding that Standard Data Protection Clauses should "be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" see 44(1)[105].

The Court held that the standard of essential equivalence – which it had found to apply to adequacy decisions in its first Schrems judgment – also applies to data transfers under appropriate safeguards[106]. This indicate that the Court views this standard as underlying the rationale of Chapter V GDPR to avoid the circumvention of EU law, and that it is likely to apply it to other data transfer situations in the future as well[107].

Although the Standard Data Protection Clauses are binding on a data exporter established in the European union and the data importer established in a third country, it is common ground that contractual clauses are not capable of binding the authorities of that third country given that the authorities are not party to the contract[108]. This could possibly undermine the

[105] C-311/18 *Schrems II* paragraph 92

[106] C-311/18 *Schrems II* paragraph 96 and Kuner, Bygrave, Docksey, Drechsler and Tosoni (2021) page 171.

[107] Kuner, Bygrave, Docksey, Drechsler and Tosoni (2021) page 121

[108] C-311/18 *Schrems II* paragraph 125

protection required from the GDPR and the protection given in Standard Data Protection Clauses.

Depending on the third country national law, there are situations where Standard Data Protection Clauses might not constitute a sufficient means of ensuring an *essentially equivalent protection* of personal data. The Court underlines that this is the case where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates[109].

Instead of making the Standard Data Protection Clauses invalid, like the adequacy decision Privacy Shield[110], the Court underline that article 46 (1) of the GDPR does not constitute an exhaustive list. Further affirming that article 45, 46 (1) and article 46(2) (c) of the GDPR, interpreted in the light of articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by the GDPR is *not undermined*.

Consequently, to not undermine the guaranteed protection of the GDPR, it may prove necessary to supplement the guarantees contained in those Standard Data Protection Clauses[111].

The Court relies particularly on Recital 109 of the GDPR, stating that "The possibility for the controller or processor to use standard data-protection clauses (…) should [not] prevent [it] from adding other clauses or additional safeguards (…) Controllers and processors should be *encouraged to provide additional safeguards* via contractual commitments that supplement Standard Data Protection Clauses."[112] (my cursives).

It is therefore the responsibility of the data importer and data exporter to verify, on a case-by-case basis, whether the law of the third country of destination ensures *essentially equivalent protection* to that under EU law, of personal data transferred pursuant to Standard Data Protection Clauses. Where necessary, *additional safeguards* must be offered[113].

---

[109] C-311/18 *Schrems II* paragraph 126

[110] See Chapter 4.2.2. of this thesis

[111] C-311/18 *Schrems II* paragraph 132

[112] C-311/18 *Schrems II* paragraph 132

[113] C-311/18 *Schrems II* paragraph 34

Where the data exporter in the EU is not able to apply adequate additional safeguards to guarantee *essentially equivalent protection* to that of the EU, the data exporter is required to suspend or end the transfer of personal data.

4.4.3 Summary

The Court in *Schrems II* stresses that depending on the third country national law, there are situations where Standard Data Protection Clauses might not constitute a sufficient means of ensuring, a *de facto* effective protection of personal data transferred to the third country concerned.

First the data exporter and the data importer need to assess the legal situation in the third country in a way they didn't need to prior to the *Schrems II* case. Secondly, it is for the data exporters and data importers to assess and determine whether it is necessary to supplement the guarantees contained in Standard Data Protection clauses with additional safeguards[114].

In the cases of remote access to data stored in the EU the data is presumably afforded protection when stored on Union jurisdiction. It is then the access from a third country that could compromise that protection. It is therefore necessary to assess whether any compromising legislation from the third country is applicable on the situation. And, if that in turn causes an undermining of the protection of the personal data in question.

To exemplify, this could be the situation where unproportionate third country surveillance laws are applicable on the personal data stored in the Union, due to the access that is granted the third country data importer.

4.5 Binding Corporate Rules

4.5.1 An introduction to Binding Corporate Rules

Binding Corporate Rules are regarded as a transfer tool under article 46(2)(b). Article 47 of the GDPR lists numerous conditions to have Binding Corporate Rules approved but does not give a clear definition. The definition is given in article 4(20) of the GDPR; Binding Corporate Rules means personal data protection policies which are adhered to by a data

[114] C-311/18 *Schrems II* paragraph 132

exporter established on the territory of a Member State for transfers of personal data to data importer in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Binding Corporate Rules are an innovation developed by the WP29, which explained that due to the complex architectural structures some multinational companies have, they would like to benefit from the possibility to adopt "codes of conduct for international transfers"[115].

The purpose of Binding Corporate Rules is that if a group of undertakings, or group of enterprises engaged in a joint economic activity, can guarantee the same data protection throughout their organisation, this can compensate for the lack of data protection laws in a third country[116]. This is reliant on that such Binding Corporate Rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers of personal data, see Recital 110 to the GDPR.

Binding Corporate Rules needs to be approved by the competent supervisory authority in accordance with the consistency mechanism set out in article 63 of the GDPR, see article 47(1). This ensures the consistent application of the GDPR throughout the Union, and cooperation between the supervisory authorities, see Recital 135. Thus, upholding the goal of harmonization behind EU legislations such as the GDPR.

The supervisory authority can only approve Binding Corporate Rules if they are legally binding, apply to and are enforced by every member concerned of the group of enterprises engaged in a joint economic activity, including their employees, see article 47(1)(a).

Moreover, Binding Corporate Rules needs to expressly confer enforceable rights on data subjects regarding the processing of their personal data, see article 47(1)(b). The last criterion of article 47(1)(c), is that the Binding Corporate Rules fulfil the requirements laid down in paragraph 2.

Article 47 Paragraph 2 contains fourteen conditions that "Binding Corporate Rules at the least shall specify". The list of conditions is not exhaustive, as is shown by the words "at least" in the text. This suggest that that the CJEU´s statement in relation to Standard Data Protection

---

[115] WP29 (2003) page 5

[116] Much like the concept of Standard Data Protection Clauses in Chapter 4.4. of this thesis.

Clauses in *Schrems II* is transferable to Binding Corporate Rules[117]. Presumably, if a data exporter applies Binding Corporate Rules, this "should [not] prevent [it] from adding other clauses or additional safeguards"[118].

An analogy like this could also find support in the fact that Binding Corporate Rules does not bind state authority, much like Standard Data Protection Clauses[119]. Consequently, implying that data exporters and data importers who solely relied on Binding Corporate Rules as a transfer tool after the *Schrems II* also would need to make a case-by-case analysis of their data transfers as well as provide for additional safeguards if necessary.

It would go too far for this thesis to address all conditions laid down in article 47(2). But I will enhance a few conditions to illustrate the content of Binding Corporate Rules.

Binding Corporate Rules shall specify the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question[120], as well as their legally binding nature, both internally and externally[121]. Binding Corporate Rules also needs to specify the application of the general data protection principles, such as legal basis for processing, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the Binding Corporate Rules[122]. They then need to specify the rights of data subjects regarding processing and the means to exercise those rights[123].

---

[117] "The possibility for the controller or processor to use standard data-protection clauses (…) should [not] prevent [it] from adding other clauses or additional safeguards (…) Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.", see Schrems II paragraph 132 and Chapter 3.2.1 of this thesis.

[118] C-311/18 *Schrems II* paragraph 132.

[119] C-311/18 *Schrems II* paragraph 125 and Chapter 4.4.2. of this thesis.

[120] Article 47(2)(b) of the GDPR

[121] Article 47(2)(c) of the GDPR

[122] Article 47(2)(d) of the GDPR

[123] Article 47(2)(e) of the GDPR

It is also worth highlighting that Binding Corporate Rules entails that the establishment on the territory of a Member State accepts the liability for any breaches of the Binding Corporate Rules by any member concerned not established in the Union[124].

4.5.2 Summary

If, on one hand it is the lack of data protection law that is the reason a data exporter cannot give remote access to data in a third country, well written and approved Binding Corporate Rules can compensate for this. In the cases of remote access to data stored in the EU/EEA, the data is given protection in storage, as well as through the access if the company that is remotely accessing the data is complying to Binding Corporate Rules who compensate for third countries lack of data protection law.

If, on the other hand, there is unproportionate interference or surveillance from state authority, Binding Corporate Rules cannot, by their very nature, bind state authority and thus cannot alone act as an "appropriate safeguard" by analogy to the *Schrems II* judgement paragraph 125.

Binding Corporate Rules can be used as an additional safeguard, but that again will depend on the reason for needing such safeguards[125].

4.6 Additional safeguards for remote access

4.6.1 Introduction

When transferring personal data to a third country based on appropriate safeguards, a data exporter and a data importer must ensure that the transfer tool in question is effective in the light of all circumstances of the transfer. Specifically, that the transferred personal data in the third country is afforded protection *essentially equivalent* to that guaranteed in the EU/EEA by the GDPR, read in the light of the Charter, see Chapter 1.3.2 and 3.1 of this thesis.

---

[124] Article 47(2)(f) of the GDPR, the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage

[125] The EDBP Recommendation (01/2020) page 36

This part of the thesis will address some of the possible additional safeguards and assess whether they could provide for *essentially equivalent protection* of personal data. This is however not meant as an exhaustive assessment of every possible additional safeguard. It is up to the data exporter and the data importer to do an individual assessment of each data transfer and identify suitable additional safeguards when necessary[126].

4.6.2 The individual assessment of each transfer

It's important to emphasize that the additional safeguards may differ depending on the specific aspects of each transfer situation.

Both the practical aspects such as, whether the data will be stored in the third country or whether there is remote access to data; format of the data transferred, *inter alia* encrypted or plain text; and the possibility that the data may be subject to onward transfers from the third country to another third country, matters[127].

Similarly, the legal aspect in the third country, whether the domestic legal order and/or practices in force align with EU standards, in particular the laws laying down requirements to disclose personal data to public authorities or granting such public authorities' powers of access to personal data, are important[128].

First, this means that the data exporter and the data importer will need to assess each transfer case and pay specific attention to relevant rules and practices insofar as they have an impact on the effective application of the contractual, organisational, or technical safeguards[129].

For example, the rule of law and other different aspects of the legal system in the third country would be relevant to assess the effectiveness of an individual's judicial redress

---

[126] C-311/18 *Schrems II* paragraph 134

[127] The EDBP Recommendation (01/2020) page 15

[128] The EDBP Recommendation (01/2020) page 15

[129] The EDBP Recommendation (02/2020) provide further clarifications on the elements which must be assessed to determine whether the legal framework governing access to personal data by public authorities in a third country, can be regarded as a justifiable interference and thus not infringing the rights of the data subject as guaranteed by GDPR art. 46

against unlawful government access to personal data, as well as the existence of a data protection law or an independent data protection authority[130].

Secondly, this also means that what is sufficient today might change in the light of both legal and technological developments and innovations. The fact that a technical safeguard is sufficient today, is not a guarantee that it will be able to provide *essentially equivalent protection* tomorrow.

In this individual assessment of each transfer, the EU standards such as article 7, 8, 47 and 52 of the Charter of fundamental rights must be used as a reference. It is important to assess whether access by public authorities is limited to what is necessary and proportionate in a democratic society and whether data subjects are afforded effective redress[131].

For this thesis, third country legislation not compatible with The Charter will hereunder be termed "problematic legislation".

The purpose of the individual analysis is to determine whether – and to what extent – the personal data is affected by any problematic legislation of a third country and whether – and to what extent – that affects the protection of that personal data. Consequently, after learning this, the data exporter and the data importer can facilitate for additional safeguards that provide satisfactory protection.

4.6.3 Contractual and organisational safeguards

4.6.3.1 Introduction

If an assessment as mentioned in Chapter 4.6.2 reveal that the personal data may fall within the scope of problematic legislation in a third country, a data exporter and a data importer may need to suspend the transfer or implement additional safeguards.

[130] The EDBP Recommendation (01/2020) page 16

[131] The EDBP Recommendation (01/2020) page 16

This Chapter of the thesis will highlight the contractual safeguards as recommended by the EDPB in their 01/2020 Recommendation. Such measures will largely consist of unilateral, bilateral, or multilateral[132] contractual commitments.

If an article 46 GDPR transfer tool is used, it will in most cases already contain several contractual commitments by the data exporter and the data importer aimed at serving as safeguards for the personal data[133].

The overlapping of contractual commitments for data importers and data exporters makes the legal landscape complicated. This may in worst case scenarios lead to data controllers and data processors who believe they have implemented additional safeguards when the safeguards in fact overlap the art. 46 transfer tools they are already relying upon. Consequently, believing that their protection of personal data is greater than it, *de facto,* actually is.

It is important to note that the contractual measures are characteristically more flexible than the technical safeguards. However, they may be less effective in practice because, although they bind the controller and the processor, they do not bind state authorities not party to the contractual commitments[134].

4.6.3.2 Transparency obligations

Transparency obligations are one of the contractual obligations given by the EDPB 01/2020 Recommendation. Transparency obligations are obligations given in the contract between the data exporter to the data importer, obliging the data importer to provide more in-depth information about governmental access to personal data, *inter alia* detail the laws and regulations in the destination country applicable to the importer and their processors that would permit access by public authority and indicate which measures are taken to prevent the

[132] Such as Binding Corporate Rules which should in any case regulate some of the measures listed, see The EDBP Recommendation (01/2020) page 36

[133] The EDBP Recommendation (01/2020) page 36

[134] See Schrems II paragraph 125 and Feedback NOYB (21.12.2020) page 13 “Many controllers and processors will prefer to add one or two easily implementable contractual measures instead of re-engineering their systems. The EDPB should highlight that adding some “light weight” contractual measures will usually not be sufficient to achieve adequate protection.”

access to transferred data[135]. A criterion for effectiveness is that the data importer can provide the exporter with this type of information.

As a measure for data exporters and data importers to comply with the individual assessment of each transfer this is a useful set of contractual obligations. Thus, giving the data exporters a sufficient foundation to base their decision of whether to transfer with additional safeguards or to suspend transfers.

It´s important to emphasize that transparency obligations could not constitute a contractual commitment equipped to ensure the essential equivalent protection of personal data.

To provide *essentially equivalent protection*, the exporter could also add clauses where the importer verifies that first, they have not purposefully created back doors or similar programming that could be used to access the system and/or personal data. Secondly, that they have not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems[136]. And finally, that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key[137].

However, it's important to emphasise that the actual protection such a clause is capable of giving is relative to the laws and practices in the third country. This could not ensure an *essentially equivalent protection* of personal data in a third country that has surveillance laws that exceeds what is necessary in a democratic society and not proportionate. Furthermore, if the legislation or government policies prevent importers from disclosing this type of information this may render this clause ineffective[138].

The data exporter could reinforce its power to conduct audits or inspections of the data processing facilities of the importer, such audit could be on-site and/or remotely. This could verify if data has been disclosed to public authorities as well as under which conditions data

---

[135] The EDBP Recommendation (01/2020) page 37

[136] The EDBP Recommendation (01/2020) page 37

[137] The EDBP Recommendation (01/2020) page 38

[138] The EDBP Recommendation (01/2020) page 38

has been disclosed under, *inter alia* if access has been beyond what is necessary and proportionate in a democratic society.

The scope of the audit should legally and technically cover any processing by the importer's processors or sub-processors of the personal data transmitted in the third country to be fully effective. Furthermore, access logs and other similar trails needs to be tamper proof so that the auditors can find evidence of disclosure if there are any. Access logs and other similar trails should also distinguish between accesses due to regular business operations and accesses due to orders or requests for access from state authorities[139].

However, for some cases of remote access in business-to-business relations, this might be troublesome for the data importer, *inter alia* if they are project-based business partners.

For these cases, an innovative method could be to reinforce the transparency obligations of the importer by providing for a "Warrant Canary" method, where the importer commits to regularly publish – e.g., at least every 24 hours – a cryptographically signed message notifying the data exporter that as of a certain date and time it has received no order to disclose personal data[140]. The absence of this notification will imply to the data exporter that the importer may have received an order. This will require the data exporter to monitor the Warrant Canary notifications.

It is also necessary for the data importer to ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by law of the third country. It is necessary to establish the law of the third country and possibly have a person outside the third countries jurisdiction issue the Warrant Canary.

4.6.3.3 Obligations to take specific actions

The data importer could commit to revise the legality of any order to disclose data under the laws of the third country. Particularly whether it remains within the powers granted to the requesting public authority, and to challenge the order if, after an assessment, it concludes that there are grounds under the law of the country of destination to do so. When challenging

[139] The EDBP Recommendation (01/2020) page 39

[140] The EDBP Recommendation (01/2020) page 40

an order, the data importer should seek interim measures to suspend the effects of the order until the court has decided on the merits.

The importer would have the obligation not to disclose the personal data requested until required to do so under the applicable procedural rules. The data importer would also commit to providing the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order[141].

Such a clause will offer limited additional protection as an order to disclose data may be lawful under the legal order of the third country, but still not comply with the EU standards. For this clause to have an effect it also requires that the legal order of the third country has effective legal remedies and avenues to challenge orders to disclose data.

Critics of this approach as an additional safeguard highlight that challenging "every government request where there is a lawful basis to do so, is nothing but a commitment to not provide data without a valid legal basis." Upholding that this is not a supplementary measure, but a direct consequence of compliance with Article 6(1) GDPR[142]. Where there is no legal basis, the controller or processor may not provide personal data to any authority.

4.6.3.4 Empowering data subjects to exercise their rights

The contract could provide that personal data transmitted in plain text in the normal course of business may only be accessed with the express or implied agreement of the exporter and/or the data subject for a specific access to data[143].

Such a clause could be effective in those situations where data importers receive requests from public authorities to cooperate on a voluntary basis. But will nonetheless not give any excess protection in the cases of data access by public authorities that happens without the data importers knowledge or against its will.

---

[141] The EDBP Recommendation (01/2020) page 40

[142] Feedback NOYB (21.12.2020) Page 14

[143] The EDBP Recommendation (01/2020) page 40

For the cases of remote access in business-to-business relations, the data subject might not be able to oppose the access or to give a consent that meets the conditions of article 4(11) of the GDPR[144].

4.6.3.5 Internal policies for governance of transfers within groups of enterprises

The adoption of adequate internal policies with clear allocation of responsibilities for data transfers and standards operating procedures are one of the safeguards outlined by the EDPB in their 01/2020 Recommendation.

The description of a "internal policy" appears a lot like that of Binding Corporate Rules. The main discrepancy is that Binding Corporate Rules are subject to the approval of European Commission and the supervisory authority, see Chapter 4.5. By analogy to Binding Corporate Rules, these policies may only be envisioned for the cases where the request from public authorities in the third country is compatible with EU law[145]. If there is surveillance by state authorities that would be considered unproportionate under EU law, internal policies will not provide protection.

It´s also important to emphasize that the data importer and the data exporter needs to assess and compare the internal policies with Binding Corporate Rules if that is the transfer tool in question. If the content internal policies overlap with the Binding Corporate Rules already in place there might not be any additional safeguarding of the personal data transferred.

4.6.3.6 Providing for the contractual obligation to use specific technical safeguards

If additional safeguards are necessary, a data exporter and a data importer is likely required to implement technical measures. As seen above, contractual and organizational measures alone will often not be sufficient to address the problematic legislation or practice[146]. This is

[144] freely given, specific, informed, and unambiguous see article 7 GDPR, and Recital 32.

[145] See Case C-362/14 *Schrems I* paragraph 94 and C-311/18 *Schrems II,* paragraphs 168, 174, 175 and 176, as well as The EDBP Recommendation (01/2020) page 44.

[146] The EDBP Recommendation (01/2020) page. 22 and The Danish Recommendation (03/2022) page 19.

however dependent on the specific circumstances of the problematic legislation or practice in the third country.

For a clause like this to be effective, there needs to be technical measures that has been identified as effective. It would then be provided in a legal form to ensure that the data importer also commits to put in place the necessary technical measures if need be.

The next Chapter will give a brief introduction of encryption and pseudonymisation as a technical safeguard.

4.6.4 Technical safeguards

4.6.4.1 Introduction

Technical safeguards are technological solutions to the legal problem of third country transfers. This will not be the focus of the thesis, but it's necessary to introduce their role in the cases of remote access in business-to-business relations.

Technical safeguards aim to exclude potential infringing access by public authorities by preventing the authorities from identifying the data subject. Or e.g., associating the transferred data with other data sets that may contain, *inter alia* online identifiers provided by the devices, applications, tools, and protocols used by data subjects in other contexts[147].

These measures could be able to guarantee an *essentially equivalent* level of protection to that guaranteed in the EU/EEA. Especially, if the access by public authorities complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society[148].

Public authorities in third countries may attempt to access transferred data in transit by accessing the lines of communication used to convey the data to the recipient country. They can either access the processing facilities themselves, or require a recipient of the data to locate, and extract data of interest and turn it over to the authorities.

---

[147] The EDBP Recommendation (01/2020) page. 29

[148] The EDBP Recommendation (01/2020) page. 29, See also C-311/18 *Schrems II* paragraph 132 and Chapter 3.2.1 of this thesis

In the EDPB letter regarding the European Cybersecurity Certification Scheme for Cloud Services, the EDPB further highlights the importance of *Schrems II* in remote access cases such as for Cloud Service providers. Noting that compliance can be reached e.g., with certain approaches to encryption and key management[149]. Clearly supporting that there needs to be a technological solution to this legal problem.

4.6.4.2 Pseudonymised and encrypted data

By article 4(5) of the GDPR "Pseudonymisation" is defined as the processing of personal data in such a manner that the "personal data can no longer be attributed to a specific data subject without the use of additional information". Moreover, such additional information must be "kept separately" and must be "subject to technical and organisational measures" to ensure that the personal data are not attributed to an identifiable natural person.

Additional information may consist of tables juxtaposing pseudonyms with the identifying attributes they replace, cryptographic keys or other parameters for the transformation of attributes, or other data permitting the attribution of the pseudonymised data to identified or identifiable natural persons[150]. A way of pseudonymise data is by way of encryption. Encryption is a process which transposes data into an unintelligible form, a process which can be difficult to reverse, without the correct decryption key.

For remote access to data, it is possible to pseudonymise data; a data exporter in the EU gives access to personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information. The additional information would also need to be subject to "technical and organisational measures" to ensure that the data remains unattributable to the data subject.

However, this makes it difficult for the data importer, if they, e.g., needs direct access to data of its own choice, and uses the data in the clear for its own purposes, *inter alia,* to perform personnel services[151]. If there is a need for data under these conditions, there are at the time

---

[149] EDPB Letter (23/11/2021)

[150] The EDBP Recommendation 01/2020 page. 31

[151] The importer has become the data controller and not simply the data processor, see Chapter 2.3.2. of this Thesis.

no technical solutions. The EDPB states that it is "incapable of envisioning an effective technical measure" for remote access to data for business purposes which requires access under such conditions[152].

Critics of this rigid approach to the cases of remote access to data highlight that it's not realistic for multinational companies to avoid access to personal data in the clear from third countries. Many multinational companies with global reach often have strongly integrated businesses using common tools for HR, sales & marketing, etc. which inevitably require an exchange of data across the globe and access to personal data in the clear[153].

Furthermore, its highlighted that the EDPB do not consider the fact that even in the cases of end-to-end encrypted services, at least some data needs to be unencrypted to provide the services e.g., connection information, session state, IP addresses, and basic subscriber data[154].

Foreign companies invested in the EU routinely transfer the human resources data of their European employees to headquarters in non-adequate jurisdictions[155]. Where problematic legislation applies to the personal data, a data exporter and a data importer would need to rely on an adequacy decision or in fact, suspend data transfers.

4.6.4.3 Summary

If, on the one hand, the processing by the data importer can suffice with pseudonymised or encrypted data, this would not constitute a breach because the personal data will also be encrypted for State Authorities, and therefore also protected. On the other hand, if problematic third country legislation applies to the transfer, and the data importers need for data in the clear – without pseudonymisation or other encryption – that would constitute a breach of article 46 of the GDPR read in the light of the Charter[156].

---

[152] The EDPB Recommendation (01/2020) page 35.

[153] Feedback DLA Piper (21.12.2020) page 2

[154] Feedback DLA Piper (21.12.2020) page 2; Feedback ITI (21.12.2020) page 6

[155] Feedback U.S. Chamber of Commerce (18.12.2020) page 5

[156] C-311/18 *Schrems II* paragraph 92

This thesis shows that there are no technical or contractual safeguards that can be implemented when, firstly, problematic legislation applies to the data transfer, and secondly, the data importer needs data in the clear, such as for HR resources.

5 A Critical perspective

Though the need for protection of personal data is bigger than ever[157], the rules and practices relating to third country transfers are right in the intersection of technology, law and international cooperation and politics. As this thesis illustrate, the legal landscape is dynamic, and this can cause compliance difficulties for businesses.

Studies show that the pitfalls of the GDPR are, *inter alia,* a regulatory burden[158], especially on small to medium businesses[159]; stifled innovation and growth for businesses[160]; as well as complexity for consumers[161]. On the field of international data transfers there has been a rapid change in the practice and understanding of the regulation. Possibly making the GDPR more intricate for businesses to comply with.

Organizations in the EU/EEA have diverted significant resources to understanding and interpreting the law's prescriptive provisions – at the expense of more meaningful privacy protection and innovation-generating activities[162]. Faced with the burden of compliance, some organizations outside of the EU/EEA have localized data flows or stopped servicing the European market entirely, consequently impacting economic growth, trade, and investment[163].

As seen in this thesis the transfer of personal data in the context of remote access to data give rise to many questions. As seen in Chapter 2, the definition of what constitutes as a transfer is poor. The definition of transfer in this thesis is built upon the statements from the EDPB and the EDPS because of the lack of other legal sources. The lack of supporting legal sources or legal sources with more authority, leave data exporters and data importers with an uncertainty

[157] Recital 6 to the GDPR

[158] The Canadian Marketing Association (2022) page 15

[159] The Canadian Marketing Association (2022) page 15

[160] The Canadian Marketing Association (2022) page 10

[161] The Canadian Marketing Association (2022) page 18

[162] The Canadian Marketing Association (2022) page 11

[163] The Canadian Marketing Association (2022) page 11

as to whether the rules and practices of the GDPR Chapter V applies to the cases of remote access.

Furthermore, as discussed in Chapter 3, the discrepancy in the standard of essential equivalence – with regards to the exception for national security in Member States versus in third countries – makes the comparison between legislation and practices in the Union and in the third country unequal and imbalanced. Consequently, expecting data importers and data exporters to identify reliable and suitable additional safeguards to provide an *essentially equivalent* level of protection based on a standard that, after all, exempt the most problematic rules and practices within the Union itself. To further complicate this, as Chapter 4.6.3 and 4.6.4 illustrate, the cases of state authority surveillance are intricate for data exporters and data importers to sufficiently protect against.

As illustrated by Chapter 4, the transfer tools require that the data exporters and the data importers use considerable resources with regards to evaluate the legal landscape in third countries as well as identifying which transfer tools are suitable.

The additional safeguards highlighted in Chapter 4.6 – all though not given a wide coverage in this thesis – provides for practical problems. The EDPB is, after all, incapable of envisioning an effective technical measure for remote access to data for business purposes which requires that the data importer is the data controller and requires access to data in the "clear"[164]. Supporting that data exporters and data importers needs an abundant of resources to comply with the requirements of the GDPR and the *Schrems II* judgement. Leaving it questionable to what extent businesses comply with third country transfer restrictions.

Thus, leaving the conclusion that the legal obstacles in the cases of remote access to data in third country transfers, needs to be solved either on a regional or international political level through adequacy decisions, or by technical solutions not yet envisioned by the EDPB.

[164] The EDPB Recommendation (01/2020) page 35.

Works cited

International agreements and treaties

ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950
The Charter	Charter of Fundamental Rights of the European Union. 2012/C 326/02. Official Journal C 326, 26.10.2012, p. 391–407
TEU	The Treaty on European Union (TEU), Maastricht, 07.02.1992. Consolidated version, Official Journal C 326, 26/10/2012 P. 0001 - 0390
TFEU	The Treaty on the Functioning of the European Union (TFEU), Rome, 25.3.1957. Consolidated version, Official Journal C 326/13, 26/10/2012 P. 0001 – 0390

EU Regulations and directives

Directive 95/46/EC, DPD	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. OJ L 281/31 P, 23.11.1995, p. 31-50.
Directive 2002/58, E-privacy	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47
Regulation 2016/679, GDPR	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. OJ L119/ 1., 4.05.2016, p. 1-88

EU implemented decisions

Safe Harbour	2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under

	document number C(2000) 2441) OJ L 215, 25.8.2000, p. 7–47
Privacy Shield	Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) OJ L 207, 1.8.2016, p. 1–112
SCC (EU) 2021/914	Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. C/2021/3972 OJ L 199, 7.6.2021, p. 31–61

Norwegian Law

The Personal Data Act (2018)	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger

Case law from the European Court of Justice

C- 101/01 *Lindqvist*	C-101/01 *Bodil Lindqvist* (2003) ECLI:EU:C:2003:596
C-317/04 and C-318/04	C-317/04 and C-318/04 *European Parliament v Council and*

	Commission (2006) ECLI:EU:C:2006:346
C-134/08 *Tyson Parketthandel*	C-134/08 *Hauptzollamt Bremen v J. E. Tyson Parketthandel GmbH hanse j.* (2009) ECLI:EU:C:2009:229
C-362/14 *Schrems I*	C-362/14 *Maximillian Schrems v Data Protection Commissioner* (2015) ECLI:EU:C:2015:650
C-623/17 *Privacy International*	C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (2020) ECLI:EU:C:2020:790
C-311/18 *Schrems II*	C-311/18 *Data Protection Commissioner V Facebook Ireland Ltd, Maximillian Schrems (2020)* ECLI:EU:C:2020:559
C-311/18 *Schrems II* Opinion	C-311/18 *Data Protection Commissioner V Facebook Ireland Ltd, Maximillian Schrems (2020)* AG Opinion. ECLI:EU:C:2020:5

Literature

Kuner (2013)	Kuner, C. (2013-05-09). *Transborder Data Flows and Data Privacy Law*: Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199674619.001.0001/acprof

-9780199674619 Assessed 23 May. 2022

Kuner, Bygrave, Docksey, Drechsler and Tosoni (2021) Kuner, Christopher and Bygrave, Lee A. and Docksey, Christopher and Docksey, Christopher and Drechsler, Laura and Tosoni, Luca, *The EU General Data Protection Regulation: A Commentary*/Update of Selected Articles (May 4, 2021). Available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645

Millard (2021) Millard, C. (2021). *Cloud Computing Law*: OXFORD UNIV PRESS, 2021.

Mæhle, Aarli (2017) Mæhle, Aarli, *Fra lov til rett.* Oslo: Gyldendal juridisk. 2nd edition. 2017.

Articles and webpages

Arrebola, Mauricio, Portilla (2016) Arrebola, Carlos and Mauricio, Ana Julia, and Jiménez Portilla, Héctor, An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union (January 12, 2016). Cambridge Journal of

Comparative and International Law, Vol. 5, No. 1, Forthcoming, University of Cambridge Faculty of Law Research Paper No. 3/2016, Available at SSRN: https://ssrn.com/abstract=2714259

Greenleaf (2012) — Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108, International Data Privacy Law, Volume 2, Issue 2, May 2012, Pages 68–92, https://doi.org/10.1093/idpl/ips006 assessed 22. April 2022

Georgiadou, de By, Kounadi (2019) — Georgiadou, Yola, Rolf A. de By, and Ourania Kounadi. "Location Privacy in the Wake of the GDPR" ISPRS International Journal of Geo-Information 8, no. 3: 157. https://doi.org/10.3390/ijgi8030157 (2019) Assessed 23 Mar. 2022

Lenaerts and Gutierrez-Fons (2014) — Lenaerts, K.; Gutierrez-Fons, J. A. (2014). To say what the law of the EU is: Methods of interpretation and the European court of justice. Columbia Journal of European Law, 20(2), 3-[vi]

Powles (2018) — Powles, J. The G.D.P.R., Europe's New Privacy Law, and the Future

of the Global Data Economy. The New Yorker, 25 May 2018.https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy assessed 03. March 2022

Svantesson (2010) — Svantesson, DJB 2010, 'Privacy, the Internet and transborder data flows: An Australian perspective', Masaryk University Journal of Law and Technology, vol. 4, no. 1, pp. 1-20. https://journals.muni.cz/mujlt/article/view/2554/2118 assessed 27. April 2022

Schwartz and Peifer (2017) — Schwartz, P.M. & Peifer, K.-N. (2017). Transatlantic data privacy law. Georgetown Law Journal. 106. 115-179. https://www.researchgate.net/publication/321964935_Transatlantic_data_privacy_law assessed 25. April 2022

The Canadian Marketing Association (2022) — The Canadian Marketing Association, Privacy Law Pitfalls: Lessons Learned from the European Union, February 2022, https://thecma.ca/docs/default-source/default-document-

library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6 assessed 03. April 2022

Guidelines and Recommendations

WP29 (2003) Art.29 Data Protection Working party, *working document: Transfers of personal data to third countries: Applying article 26(2) of the EU data protection directive to Binding Corporate Rules for international data transfers*, 11639/02/EN, WP 74, 3 June 2003 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

EDPS (2014) European Data Protection Supervisor, "*Transfer of personal data to third countries and international organisations by EU institutions and bodies"* Position paper, Brussels, 14. July 2014 https://edps.europa.eu/data-protection/our-work/publications/papers/transfer-personal-data-third-countries_en

WP29 (2017) Art 29 Data Protection Working Party, *'Adequacy Referential'* (Adopted 28 November 2017, as

	last Revised and Adopted 6 February 2018) WP 254rev.01, 18/EN 28. https://webcache.googleusercontent.com/search?q=cache:qz03vIIbQwsJ:https://ec.europa.eu/newsroom/article29/redirection/document/57550+&cd=1&hl=no&ct=clnk&gl=no&client=safari
EDPB Guidelines (03/2018)	EDPB Guidelines (03/2018) on the territorial scope of the GDPR (Article 3). Version 2.1 12 November 2019. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf assessed 29th of March 2022
EDBP Recommendation (01/2020)	EDBP Recommendations (01/2020) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf assessed 29th of April 2022

EDBP Recommendation (02/2020)	The EDBP recommendation (02/2020) on the European Essential Guarantees for surveillance measure from 10 November 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf assessed 29th of April 2022
EDPB Guidelines (05/2021)	The EDPB Guidelines (05/2021) on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. Adopted on 18 November 2021.https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplayChapter v_article3_adopted_en.pdf assessed 30th of April 2022
Danish DPA Guidelines (07/2021)	The Danish Data Protection Authority guidelines «Overførsel af Persnoplysninger til tredjelande" adopted July 2021, 3rd Edition. https://www.datatilsynet.dk/Media/637626336767031457/Datatilsynet_Overførsel_til_tredjelande_V3_1.0_juli2021.pdf assessed 29th of April 2022

Danish DPA Guidelines (03/2022) — The Danish Data Protection Authority guidelines "Guidance on the use of cloud", Datatilsynet Danmark, 03/2022. https://www.datatilsynet.dk/Media/637824109172292652/Vejledning om cloud.pdf assessed 29th of March 2022

EDPS Annual report 2021 (2022) — EDPS Annual report 2021, April 2022, Waterford, Ireland – Brussels, Belgium: Trilateral Research Ltd, Vrije Universiteit Brussel, 2022. ISSN 1830-9585 doi: 10.2804/146741 https://edps.europa.eu/system/files/2022-04/2022-04-20-edps_annual_report_2021_en.pdf Assessed 21st of April 2022.

Letters, Statements, Opinions and Communication

COM (2012) 0011 — Albrecht, J. P., Committee on Civil Liberties, Justice, and Home Affairs, 'Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011 –

C7-0025/2012 – 2012/0011(COD))' (2013), amendment 86. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

EDPS Opinion (2012) — EDPS, (2012) 'Opinion on the data protection reform package' https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf assessed 27th of March 2022

EDPB Statement (01/2022) — Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework Adopted on 6 April 2022 https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf

EDPB Letter (23/11/2021) — EDPB letter to ENISA regarding the European Cybersecurity Certification Scheme for Cloud Services (EUCS), 23. November 2021. https://edpb.europa.eu/system/files/2021-

	11/edpb_letter_to_enisa_out2021-00157.pdf

Feedback to the EDPB

Feedback U.S. Chamber of Commerce (18.12.2020)	U.S. Chamber of Commerce Response to the European Data Protection Board's Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with EU Level of Protection of Personal Data. Feedback 18 December 2020. R01/2020-0063. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/us_chamber_submission_edpb_supplementary_measures_final.pdf
Feedback NOYB (21.12.2020)	NOYB Comments on EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Feedback 21 December 2020. R01/2020-0169. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/noybs_comments_on_edpb_guidance_on_additional_measures_final_.pdf

Feedback DLA Piper (21.12.2020)	DLA PIPER Comments on EDPB Recommendations 01/2020 on Measures That Supplement Transfer Tools To Ensure Compliance With The EU Level of Protection Of Personal Data. Feedback 21 December 2020. R01/2020-0107. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020_12_21_dla_piper_response_to_edpb_recommendations_final3176052.1.pdf
Feedback ITI (21.12.2020)	Information Technology Industry Council (ITI Belgium) Comments to the European Data Protection Board (EDPB) Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data. Feedback 21 December 2020. R01/2020-0097 https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/iti_comments_to_the_edpb_supplementary_measures_final.pdf