Exporting data protection law

The extraterritorial reach of the GDPR

William Höglund
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviations</td>
<td>4</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Terminology</td>
<td>6</td>
</tr>
<tr>
<td>1.2 Purpose</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Delimitations</td>
<td>7</td>
</tr>
<tr>
<td>1.4 Methodology and sources</td>
<td>7</td>
</tr>
<tr>
<td>1.4.1 What is the territorial scope of the GDPR?</td>
<td>7</td>
</tr>
<tr>
<td>1.4.2 What are the legal instruments provided for by the GDPR to extend jurisdiction?</td>
<td>8</td>
</tr>
<tr>
<td>1.4.3 What types of jurisdiction and jurisdictional bases does the GDPR reflect?</td>
<td>8</td>
</tr>
<tr>
<td>1.4.4 Analysis</td>
<td>11</td>
</tr>
<tr>
<td>2 The General Data Protection Regulation</td>
<td>12</td>
</tr>
<tr>
<td>2.1 Data protection emerges in Europe</td>
<td>12</td>
</tr>
<tr>
<td>2.2 Data Protection in the EU</td>
<td>13</td>
</tr>
<tr>
<td>2.3 The material scope of the GDPR</td>
<td>15</td>
</tr>
<tr>
<td>2.4 The actors of the GDPR</td>
<td>16</td>
</tr>
<tr>
<td>2.4.1 Beneficiaries of the GDPR</td>
<td>16</td>
</tr>
<tr>
<td>2.4.2 Controllers</td>
<td>17</td>
</tr>
<tr>
<td>2.4.3 Processors</td>
<td>18</td>
</tr>
<tr>
<td>2.4.4 Enforcement</td>
<td>18</td>
</tr>
<tr>
<td>2.5 The territorial scope of the GDPR</td>
<td>19</td>
</tr>
<tr>
<td>2.5.1 In the context of activities of an EU establishment</td>
<td>21</td>
</tr>
<tr>
<td>2.5.2 Data processing in the context of activities</td>
<td>22</td>
</tr>
<tr>
<td>2.5.3 Targeting data subjects in the EU</td>
<td>23</td>
</tr>
<tr>
<td>2.5.4 Monitoring data subject behaviour</td>
<td>24</td>
</tr>
<tr>
<td>2.6 Data transfers to third countries</td>
<td>24</td>
</tr>
<tr>
<td>2.6.1 The trouble with consent</td>
<td>25</td>
</tr>
<tr>
<td>2.6.2 Adequacy decisions</td>
<td>26</td>
</tr>
<tr>
<td>2.6.3 EU – U.S. Privacy Shield</td>
<td>27</td>
</tr>
<tr>
<td>2.6.4 Standard Contractual Clauses</td>
<td>29</td>
</tr>
<tr>
<td>2.6.5 Binding Corporate Rules</td>
<td>30</td>
</tr>
<tr>
<td>2.6.6 Codes of Conduct and Certification</td>
<td>32</td>
</tr>
</tbody>
</table>
2.6.7 Derogations for particular situations .................................................. 32
2.6.8 Representatives of non-EU entities ..................................................... 33
2.7 Brief summary .......................................................................................... 33

3 Sovereignty, jurisdiction and territory in data protection ............................ 34
3.1 Sovereignty and territory .......................................................................... 34

4 Types of jurisdiction .................................................................................. 36
4.1 Prescriptive and adjudicative jurisdiction ................................................ 37
4.2 Enforcement jurisdiction ......................................................................... 37

5 Jurisdictional bases .................................................................................... 38
5.1 Territoriality principle .............................................................................. 40
  5.1.1 Subjective territoriality principle ........................................................ 41
  5.1.2 Objective territoriality principle, effects principle and passive personality principle ................................................................. 41
  5.1.3 The targeting principle ....................................................................... 42
5.2 Other permissive principles ..................................................................... 44

6 Analysis ....................................................................................................... 46
6.1 The prescriptive and enforcement jurisdiction of the GDPR .................... 47
6.2 Extending prescriptive jurisdiction .......................................................... 49

Table of References ....................................................................................... 52
Bibliography ..................................................................................................... 52
Table of Cases .................................................................................................. 57
  European Court of Justice ......................................................................... 57
  European Court of Human Rights ............................................................. 58
  International Court of Justice and Permanent Court of International Justice .... 58
  Other ........................................................................................................... 58
Table of Authorities ......................................................................................... 59
Reports and other documents .......................................................................... 59
  European Union .......................................................................................... 59
  European Data Protection Board (Article 29 Working Party) ...................... 60
  Miscellaneous .............................................................................................. 61
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>BCR-C</td>
<td>Binding Corporate Rules for Controllers</td>
</tr>
<tr>
<td>BCR-P</td>
<td>Binding Corporate Rules for Processors</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>Directive</td>
<td>Data Protection Directive</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention of Human Rights</td>
</tr>
<tr>
<td>ECJ</td>
<td>European Court of Justice</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PCIJ</td>
<td>Permanent Court of International Justice</td>
</tr>
<tr>
<td>SCC</td>
<td>Standard Contractual Clauses</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>USA/US</td>
<td>United States of America</td>
</tr>
<tr>
<td>WP</td>
<td>Article 29 Working Group Working Paper</td>
</tr>
</tbody>
</table>
1 Introduction

Personal data flows are an omnipresent occurrence in today’s globalised world and an important asset in the global economy. The interface in which data transfers take place – cyberspace – of which the Internet is by far the most widely used, crosses borders continuously. Personal data can consequently spread rapidly across the globe. In order to protect the personal data of data subjects in the European Union (EU), the EU legislator has adopted the General Data Protection Regulation (GDPR). The GDPR assign significant burden to organisations in the collection, use, disclosure, and the cross-border transfer of personal data. Not following these rules might result in heavy penalties. The GDPR has also been equipped with a broad territorial scope, which makes it possible to exercise jurisdiction beyond the territories of the EU. Consequently, significant obligations are put on entities that do not fall under the territorial jurisdiction of the EU, but are instead located inside the territories of sovereign States outside the EU. Establishing authority over entities in non-EU territories can be construed as an encroachment on the sovereignty of non-EU States. The EU’s central position in the world economy enables this behaviour of transposing EU data protection law around the world. This is done in two primary ways; by demanding that non-EU States conform to EU data protection standards, and similarly requiring that private entities that wish to have access to the EU-market complies with the GDPR. The jurisdiction of EU data protection law is thus seemingly all-encompassing. The question is if this is valid according to international law, and if not, how the GDPR bypasses certain rules of international law.

In order to concretise the impact the GDPR has on entities globally, three practical examples will be established. The examples will be revisited in Section 6 of the essay, and the reader is advised to keep them in mind throughout the essay.

Example A

*Company X is a multinational company with its main office in a third country. Company X has subsidiaries situated in several member states of the European Union. Company X transfers personal data from the European Union to its main office in the third country regularly.*

---

2 The public Internet is used by approximately 48 % of the total world population, whereas the in developed countries the figure is 81 % [https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf] retrieved 2019-01-03.
3 Svantesson, 2013, p. 92.
4 See section 2.4.4. below.
Example B

Company X is situated inside a member state of the European Union. Company Z is situated inside a third country. Company X transfers personal data for processing purposes to Company Z, which Company Z subsequently transfers back to Company X.

Example C

Company X and Company Z are both situated inside a third country. Company X has several customers in EU member states and collects personal data on individuals inside member states of the EU. Company X transfers data to Company Z for processing purposes.

1.1 Terminology

The regulation of the collection and processing of personal data have been given diverse names across the world. In U.S. legal discourse, this field of law is most commonly known as Information Privacy or simply Privacy, whereas in Europe the ordinary term is Data Protection. I will use the term data protection as this essay is overwhelmingly concerned with European data protection law. In addition, the terms cross-border and transborder will be used interchangeably. The usage of the words in legal literature is fully convergent.

1.2 Purpose

The purpose of this essay is to analyse the relation between the territorial scope of the GDPR and prescriptive and enforcement jurisdiction in customary international law, and how the voluntary compliance tools available in the GDPR are able to bypass the requirements of exercising enforcement jurisdiction. The purpose will be answered with the help of the following questions:

1. What is the territorial scope of the GDPR?
2. What are the legal instruments provided for by the GDPR to extend jurisdiction?
3. What types of jurisdiction and what jurisdictional bases does it reflect?

---

5 Bygrave, 2014, p. 23 et seq.
6 The term 'Data Protection' is derived from the German word 'Datenschutz', see Bygrave, 2014, p. 26. See also Kuner, 2013, p. 20.
8 For the use of cross-border, see for instance Voigt & von dem Bussche, 2017. For transborder, see Kuner, 2013.
1.3 Delimitations

In this essay the data protection rules of the GDPR will not be discussed in detail. Only the rules impacting jurisdiction, i.e. the territorial scope and third country data transfers, including the placement of responsibility and liability will be examined.

1.4 Methodology and sources

The method and sources used will be described according to which question it corresponds to. However, I would like to begin with a general description of how I approached the methodology and sources. The first part of the essay primarily concerns the provisions of the GDPR. The idea was that the subject of data protection and jurisdiction as a result could be grounded in the positive law\(^9\) of the GDPR. This could then be used to reflect the more complicated customary international law. Sources were located by starting in the principal works in the field. My choice consisted mainly of works by Svantesson, Kuner, Bygrave, Ryngaert, Tsagourias, Kohl and Voigt & von dem Bussche. Works authored by them were used as reference works to find further legal literature. The following subsections will describe the methodology and sources of the three questions that are to be answered to fulfil the purpose of the essay.

1.4.1 What is the territorial scope of the GDPR?

This section starts with a relatively brief narration of the emergence of data protection in Europe and its development in the context of the European Union. This meant consulting several international treaties on privacy and data protection. Legal literature were consulted in order to explain the impact of the treaties on the development of EU data protection law. This section also touches on the economic foundation of the EU, which were set in contrast to the individual rights of the EU.

Before exploring the territorial scope of the GDPR I thought it was important to identify the entities and conduct the GDPR seeks to regulate. This was done to distinguish how the scope of the GDPR impacts entities and the activities they perform,\(^10\) thus determining key concepts used in the GDPR’s terminology. In addition, the enforcement faculties in the GDPR were briefly explained, to reflect the force with which the application of the GDPR may impact entities. Thus the consequences of noncompliance was given a brief but important explanation. The use of primary sources were supplemented by secondary sources in the shape of the

\(^9\) Law that has been posited in one manner or another; adopted, passed, promulgated or enacted to provide a few examples.

\(^10\) WP 179, p. 8. See WP 169.
interpretations and reflections made in legal literature to clarify what the primary sources expresses. The interpretation of the primary sources were relatively restrictive. The secondary sources were used to reveal an approach beyond the primary sources, still being restrictive in the interpretation of EU data protection law. Books in legal literature concerning the GDPR are relatively scarce. Thus, the principal secondary source used in this context is authored by Voigt & von dem Bussche, as it covers the entirety of the regulation. Nonetheless there exist an abundance of articles and comments on the GDPR and the proposal, which were also consulted. As previously stated, references made in relation to the Data Protection Directive (Directive) are applicable to the GDPR too. Works analysing relevant provisions under the Directive were thus also used, under the consideration that the legislative text have been altered. The most important change in relation to the purpose of this essay is the change in the territorial scope of EU data protection law. The relevant case law, opinions and secondary sources were thus used to distinguish the specifics of elements in the relevant conditions in the GDPR as far as they have been explored in for instance previous judgments of the European Court of Justice (ECJ).

1.4.2 What are the legal instruments provided for by the GDPR to extend jurisdiction?

The GDPR provides for ways in which States and entities outside the EU can achieve similar data protection standards. The legal bases for executing such data transfers were examined here, and how these legal bases are used and their impact on other States and private entities. Private entities are given a selection of voluntary compliance instruments to ensure adherence with EU data protection law. The impact on States and private entities through the legal bases and the voluntary compliance options were also discussed in the context of the global economic power of the EU, touching on the Brussels effect. Regarding sources, largely the same sources as was used in answering the first question was consulted. The sources thus consisted of EU primary sources; the legislative text, the recitals, case law, and the opinions and guidelines of the EDPB, of additional secondary sources. Legal literature were consulted in order to gather information concerning the global impact of EU data protection law.

1.4.3 What types of jurisdiction and jurisdictional bases does the GDPR reflect?

In relation to this question it is important to explain why customary international law was chosen. This is connected to the sources of international law. The legal instrument generally recognised as holding the most authority in describing the sources of international law is Article
38 of the Statute of the International Court of Justice.\textsuperscript{11} The majority of authors and commentators seem to be in agreement that Article 38 presents the complete selection of the sources of international law, at least as a sensible place to start. Some have expressed reservations about the completeness of the article, seeing as the Article does not refer to resolutions of major international organizations.\textsuperscript{12} Two main sources according to Article 38 are international treaties\textsuperscript{13} and ‘International custom, as evidence of a general practice as accepted as law’.\textsuperscript{14} There are no binding international treaties on data protection.\textsuperscript{15} Customary international law then becomes a strong candidate for determining a national legislation’s adherence to public international law, as it is generally recognised that customary international law is binding on all States.\textsuperscript{16} Further connection is made in EU case law, which claims that EU law ‘is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union’,\textsuperscript{17} thus the EU is bound by international custom.

This section began by deriving jurisdiction from the concept of sovereignty, first by determining with precision the meaning of the often conflated terms ‘sovereignty’ and ‘jurisdiction’. This is followed by a description of the connection between sovereignty and territory as described by mostly secondary sources. An attempt were made to describe the technological interface in which data transfers take place and how that technology relates to sovereignty and territory. I chose to define the world in which data transfers take place as ‘cyberspace’. This definition were based on works authored primarily by Tsagourias and Tabansky. Cyberspace was then analysed in relation to territory, which as established is closely linked with sovereignty. The most important case in any discussion concerning jurisdiction in public international law is the Lotus case, which is still the only international court judgment which examines jurisdiction specifically,\textsuperscript{18} and from which the jurisdictional types can be discerned.\textsuperscript{19} The jurisdictional principles of public international law consists of the \textit{jurisdictional types}: (1) prescriptive jurisdiction; (2) adjudicative jurisdiction; and (3)

\begin{itemize}
\item \textsuperscript{11} Svan
\item \textsuperscript{12} Svan
\item \textsuperscript{13} Article 38.1 Statute of the International Court of Justice.
\item \textsuperscript{14} Article 38.2 Statute of the International Court of Justice.
\item \textsuperscript{15} Bygrave, 2014, p. 205-206.
\item \textsuperscript{16} Thirlway, 2010, p. 102.
\item \textsuperscript{17} Case C-366/10, \textit{Air Transport Association of America and others}, 2011. As shown in the quotation above, the particular circumstances in the case referred was that of the applicability of international customary law.
\item \textsuperscript{18} Ryngaert, 2008, p. 4. Lowe & Staker, 2010, p. 318.
\item \textsuperscript{19} The Case of the SS Lotus, No. 18-19. Lowe & Staker, 2010, p. 318.
\end{itemize}
enforcement jurisdiction,\textsuperscript{20} and of the \textit{jurisdictional bases}.\textsuperscript{21} It is doubtful that adjudicative jurisdiction is necessary to single out in relation to EU data protection law, as the prescriptive situation will lead to the same result,\textsuperscript{22} which is why adjudicative jurisdiction was treated under the same banner as prescriptive jurisdiction.

The jurisdictional bases were compared to the territorial scope of the GDPR in order to determine which bases the regulation uses as legal justifications for its jurisdiction, with focus lying on the territoriality principle. The resulting jurisdictional bases were then analysed further in order to determine their properties and use mostly in relation to the GDPR. The jurisdictional bases were also discussed in the Lotus case, but the basic framework used in this essay consists of the Harvard Draft,\textsuperscript{23} which lists and describes permissive principles of customary international law, and is generally used in legal literature.\textsuperscript{24} Overall, in answering this question I made heavy use of legal literature in order to shed light on otherwise large, complex and abstract concepts.

Another important matter is how the question of jurisdiction in public international law affects private parties. Public international law and private international law are generally viewed as two distinct legal fields; public international law governs the relations between States, and private international law governs the relationships between individuals.\textsuperscript{25} On an increasingly frequent basis, authors and commenters have viewed the principal jurisdictional issues of data transfers as one single issue, shedding the conventional dichotomy of public and private, as individuals has become subjects of public international law.\textsuperscript{26} Public international is the basic delimiting standard of the international legal order,\textsuperscript{27} which means that it also places a degree of limits onto international private law.\textsuperscript{28} The interactions between States in the framework of public international law affects private parties. According to the Working Party, the question of applicable law and jurisdiction is a question for public international law.\textsuperscript{29} The extraterritorial effects of EU data protection law makes it appropriate to discuss from the view of public international law jurisdictional rules.

\begin{itemize}
\item \textsuperscript{20} Lowe & Staker, 2010, p. 316-318, 335.
\item \textsuperscript{21} Generally accepted jurisdictional bases are the territoriality principle, personality principle, protective principle and universality principle, see Lowe & Staker, 2010, p. 315. See also below at section 5.
\item \textsuperscript{22} Kuner, 2010, p. 184. See Lowe & Staker, 2010, p. 317.
\item \textsuperscript{23} Harvard Draft, 1935.
\item \textsuperscript{24} See Ryngeart, 2008; Svantesson, 2013.
\item \textsuperscript{26} Svantesson, 2013, p. 36. Kohl, 2015, p. 32.
\item \textsuperscript{27} Kuner, 2010, p. 183-184. WP 56, p. 2. See Kohl, 2015, p. 32.
\item \textsuperscript{28} Kohl, 2015, p. 32.
\item \textsuperscript{29} WP 56, p. 2. See Kuner, 2010, p. 184.
\end{itemize}
The GDPR contains both public and civil provisions. In the GDPR, a regulatory breach might result in both a civil matter, a compensation claim\(^\text{30}\) and an administrative fine\(^\text{31}\) enforced by the regulatory authorities. It would seem strange that international law on jurisdiction would govern the latter claim but not the former, as the two activities arose out of the same conduct and required the same compliance by the entity impacted by the enforcement.\(^\text{32}\) The GDPR also contains ways of bypassing traditional jurisdictional rules in public international law by providing private law instruments through a legal instrument that is probably most similar to public law, thereby binding private parties to the data protection legislation of one State. Furthermore, the GDPR applies to personal data belonging to data subjects in the EU even after it has exited the territory of the Union. It is thus not simply a choice of laws; the regulation applies to personal data that has undergone contractual transfer, and is thus in another State’s jurisdiction, under that State’s sovereignty.

Moreover, EU data protection law has a strong connection to human rights.\(^\text{33}\) To protect the rights conferred onto data subjects in the EU, the reach of the GDPR is wide. It thus not only impacts private parties operating in the EU, but also their operations in States not part of the EU. This can be viewed as an infringement on the sovereignty of those States. This then becomes a matter of State-to-State interaction, which is in the area of public international law.\(^\text{34}\) Furthermore, the reach of the GDPR means that the provisions will attach themselves to entities having some kind of data processing interaction with data subjects in the EU. Thus, it would seem appropriate to treat the GDPR as an instrument which puts limits on private entities as an effect of the jurisdictional types in public international law.

1.4.4 Analysis
In the final part of the essay the positive law of the GDPR were analysed in relation to the jurisdictional principles in customary international law. This meant analysing how jurisdiction is permitted under prescriptive and enforcement jurisdiction, and how the voluntary compliance tools available in the GDPR are able to bypass the requirements of exercising enforcement jurisdiction. The jurisdictional principles, i.e. the interaction between the jurisdictional types and the relevant jurisdictional base (the territoriality principle) were analysed in relation to the interplay between jurisdiction and sovereignty.

\(^{30}\) Article 82 GDPR.
\(^{31}\) Article 83 GDPR.
\(^{32}\) Kohl, 2015, p. 32-33.
\(^{33}\) See Kuner, 2013, p. 21.
\(^{34}\) Svantesson, 2013, p. 36.
2 The General Data Protection Regulation

2.1 Data protection emerges in Europe

In the 1970’s data protection emerged as a separate field of law in relation to privacy law. The new field arose as a consequence of ever increasing growth in information technology and rapid globalization. Following the enactment of national data protection acts, discussion continued in the international context, where the protection of human rights also came into view as cause for new regulation. The Organization for Economic Cooperation and Development (OECD) adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, which was quickly followed by the Council of Europe (CoE) who adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Shifting from mostly national interests, both the OECD and the CoE recognized that transborder flow of data was increasing, and that it was competing value to privacy, a line of thought that can be traced to the Directive and the GDPR. The CoE was highly influential in the European development of data protection law, and is largely the forebear to the EU-wide Directive. The principles developed in Convention 108 functioned as the foundation for all subsequent European data protection regulation. The ratification of C-108 was furthermore supported by the EU and has currently been ratified by all EU member states.

37 Concerning cross-border flows of data, Chapter 3 of the Convention contains rules on data transfers between parties of the convention. Article 12.2 holds the primary provision, and holds that a party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another party. Nevertheless, parties are permitted to derogate from the main rule, in accordance with Article 12.3a, which stipulates that a party may derogate from Article 12.2 insofar as the data in question are specifically protected in the party’s legislation and the other party does not offer equivalent protection. See Bygrave, 2014, p. 38 and Birnhack, 2008, p. 511.
38 OECD Guidelines para. 17: member countries should refrain from restricting transborder flows of personal data between itself and another country. The accountability principle is also a prominent feature of the OECD Guidelines (a controller remains accountable for personal data under its control without regard to the location of the data, OECD Guidelines para. 16.). See further Kuner, 2013, p. 32 et seq. and Bygrave, 2014, p. 44 et seq., and Birnhack, 2008, p. 511.
40 González Fuster, 2014, p. 92.
42 Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. See also González Fuster, 2014, p. 93.
2.2 Data Protection in the EU

Achieving sufficient data protection and trade liberalization in the EU were and still are inseparable aspirations. This is not however because data protection and free trade are natural counterpoints, but for political reasons. Nevertheless, some commenters argue that they are two sides of the same coin, in that sufficient data protection is required to maintain a free flow of data. An extensive list of fundamental rights exist in the law of the EU. The only way to achieve a free flow of information, and thus trade liberalization, was to ensure that these fundamental rights were protected. EU data protection thus attempts to provide a balance between the free flow of data, and the protection of the fundamental rights and freedoms of natural persons.

In the 1990’s the EU decided to enter the data protection field which resulted in the Data Protection Directive of 1995, which was largely based on the OECD Guidelines and Convention 108. The Directive was the most comprehensive data protection instrument to date, and was greatly significant in globalizing data protection with extraterritorial effects. Consequently, EU data protection law has had significant influence on other States’ data protection regulation. One detailed analysis of EU influence on data protection and privacy regulation found that 29 out of 33 non-European data protection regulations shared four out of ten key features with the relevant EU legislation. Interestingly, each and every one of the ten key features were found in 13 non-European data protection laws.

The purpose of the Directive was ‘to protect the fundamental rights of individuals, and in particular the right to privacy, which was an aim not borrowed from national European legislation but from Convention 108. The object of the Directive was not expressly the protection of personal data, but focused on the protection of individuals with regard to the processing of personal data. In addition, the protective objective of the Directive was to oblige...
EU member states to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy. Case law further confirmed the connection between the Directive and Article 8 European Convention of Human Rights (ECHR). A key development was the incorporation of a data protection provision into the Lisbon Treaty. Thus, data protection has emerged as an EU fundamental right, which is visible in the EU Charter of Fundamental Rights, the ECHR, and in the common national constitutional traditions of EU member states.

In 2016 the GDPR was adopted to replace the Directive and the regulation went into force in 2018. The aim of the GDPR was to strengthen the protection of individuals in relation to positive fundamental rights given in Article 16 of the Treaty of the Functioning of the European Union (TFEU) and Article 8 of the Charter of Fundamental Rights of the European Union. From a practical view, the need for renewal of EU data protection stemmed from the fragmentation of data protection regulation across the Member states of the EU, which resulted in an irregular application of EU data protection law across the Union, thus distorting the competition in the internal market. It lies in the legal nature of an EU regulation that it applies directly to its beneficiaries and does not require national implementation by the member states. The GDPR takes aim at strengthening legal certainty to facilitate the free flow of data by treating personal data responsibly, in order to promote the EU digital economy. In the GDPR, the EU legislator has recognized the current rapid technological developments and

---

58 Joined Cases C-465/00, C-138-01 and C-139/01, Österreichischer Rundfunk and Others and C-101/01, Lindqvist.
60 Article 6.2 TFEU in connection with Article 8 of the Charter. This meant that the Charter was now legally binding. See Gonzalez Fuster, 2014, p. 192.
61 Article 6.2-3 TFEU in connection with Article 8 ECHR. Case law has given the right of privacy a broad interpretation, see Gonzalez Fuster, 2014, p. 95 and Nardelli, 2010, p. 46. For relevant cases see in particular Leander v. Sweden; S. and Marper v the United Kingdom. Gonzalez Fuster, 2014, p. 170-171. The European Court of Justice references the ECHR and its associated case law, see for instance C-136/79, National Panasonic and C-369/98, Fisher.
63 Article 99 GDPR.
64 GDPR rec. 1.
66 Article 288 TFEU. See Reding, 2012, p. 121.
68 GDPR recs. 7, 9 GDPR.
globalization and the challenges it brings to international data transfers.\textsuperscript{70} As a result the scope of application is very wide, one which will affect countless entities globally.\textsuperscript{71}

2.3 The material scope of the GDPR

To ensure a high level of protection, the material scope is assumed to be interpreted very broadly.\textsuperscript{72} In order to discuss the territorial scope of the GDPR and its implications, a brief description of the persons and subject matter that relates to the GDPR.

**Personal Data.** In this context, data means electronically stored information, ‘signs or indications.’\textsuperscript{73} In terms of the GDPR, data has to be *personal* in nature to fall under its scope of application. *Personal data* is electronically stored information relating to an identified or identifiable natural person.\textsuperscript{74} This individual is known as the *data subject*.\textsuperscript{75} Data is deemed to qualify as *personal* if it is possible to identify a data subject on the basis of the available data. In other words, if it is possible to detect the identity of a person directly or indirectly.\textsuperscript{76} Data is thus *personal* if it is possible to assign a *characteristic* that carries an expression of a physical, physiological, psychological, genetic, economic, cultural or social identity.\textsuperscript{77} Examples of identifiers are, e.g., personal names, identification numbers (social security numbers, identification (ID) numbers etc.), location data and online identifiers.\textsuperscript{78} Online identifiers include Internet Protocol (IP) addresses, cookies or other activities that can be traced and carries identification tags.\textsuperscript{79} Personal data then, is the result of the possibility of identification, the ‘identifiability’, and does not require clear identification of an individual. Identification of an individual is the result of a combination of different sources of information, where the separate pieces of information does not in themselves provide a sufficient connection to the individual, but does so in combination.\textsuperscript{80}

**Processing.** The term processing as used in the GDPR means any operation or set of operations which is performed on personal data or sets of personal data.\textsuperscript{81} This means that any

\textsuperscript{70} GDPR rec. 6.
\textsuperscript{72} Voigt & von dem Bussche, 2017, p. 5.
\textsuperscript{73} Voigt & von dem Bussche, p. 11. See Bygrave, 2014, p. 126.
\textsuperscript{74} Article 4.1 GDPR.
\textsuperscript{76} Ibid.
\textsuperscript{77} Article 4.1 GDPR. See Voigt & von dem Bussche, 2017, p. 11.
\textsuperscript{78} Article 4.1 GDPR. See Voigt & von dem Bussche, 2017, p. 11.
\textsuperscript{79} GDPR rec. 30. See Voigt & von dem Bussche, 2017, p. 11.
\textsuperscript{81} Article 4.2 GDPR.
handling or treatment of data will be considered as processing within the scope of application, whether it involves collecting, recording, organizing, structuring, storing or erasing data. Examining prior legislation yields similar results; judging by how processing was considered in the Directive, the term is likely limitless. The list of operations that constitute processing indicate that the list of operations is not exhaustive. The term processing as used in the GDPR encompasses basically any use of personal data.

**Accountability.** The GDPR contains a general accountability principle, which means that primarily controllers are obligated to ensure compliance with the GDPR, which also includes that the burden of proof are placed on the controller. The accountability refers to the adherence of the entity to the data processing principles laid out in the GDPR.

### 2.4 The actors of the GDPR

The personal jurisdiction of the GDPR consists of controllers, processors, and individuals who benefit from the data protection the GDPR sets out to solidify. The actual form of the legal person is irrelevant. To fall under the scope of application of the GDPR, instead conditions of role and obligations for data security are considered.

#### 2.4.1 Beneficiaries of the GDPR

The GDPR provides protection for all individuals, regardless of nationality or residence. Thus it does not limit the application of the regulation to processing of personal data of individuals who are in the EU. Any data processing that falls under the scope of application, irrespective of the location or the nationality of the data subject is covered by the GDPR.

**Legal entities.** As a general rule, irrespective of legal form, legal persons are not beneficiaries of the protection granted by the GDPR. Of course, there are exceptions: the data belonging to legal persons could be regarded as personal data if it includes information on individuals associated with the legal entity. The other exception is one-man companies. They

---

83 Voigt & von dem Bussche, p. 10; Lloyd, 2014, p. 52. See for instance C-101/01, Lindqvist. The Advocate General dissented from the opinion of the Court, see C-101/01, Opinion of Advocate General Tizzano.
86 Article 5.2 GDPR.
87 See WP 173.
88 Article 1.1 GDPR in connection with GDPR, rec 14.
89 EDPB, Guidelines 3, p. 9.
are considered natural persons as it was not deemed possible to isolate corporate data from data of personal nature.\(^\text{92}\)

### 2.4.2 Controllers

Controllers are the primary targets of the accountability principle\(^\text{93}\) and carries general responsibility and liability for any processing of personal data performed by itself or on its behalf.\(^\text{94}\) A controller is defined as a natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the processing of personal data.\(^\text{95}\) This definition is identical to the one which was given in the Directive. Thus, there are three primary components: (1) a natural or legal person, public authority, agency or other body; (2) that alone or jointly with others; (3) determines the purposes and means of data processing.\(^\text{96}\)

A natural or legal person. The legal form of the controller is irrelevant concerning the personal scope of application of the GDPR. Furthermore, the GDPR does not contain an intra-group exemption. Within a business group structure, each individual company is responsible for any data processing occurring inside its control. Each company is thus considered a controller.\(^\text{97}\)

That alone or jointly with others. The GDPR provides for clear allocation of responsibilities known as joint controllers.\(^\text{98}\) In situations where two or more controllers determine the purpose and means of processing by several entities collectively, for instance subsidiaries within a business group structure, obligations stemming from the GDPR are to be shared amongst them. Furthermore a clear allocation of those responsibilities must be shown to exist. Controllership comes in a wide array of shapes, where various parties may interact or be connected to each other in different ways by processing personal data.\(^\text{99}\) Generally speaking, a controller exhibits behaviour that demonstrates an independence in relation to contracting partners and in deciding the purpose of the data processing.\(^\text{100}\)

---

\(^\text{93}\) Article 5.2. GDPR.
\(^\text{94}\) Article 24 GDPR.
\(^\text{95}\) Article 4.7 GDPR.
\(^\text{98}\) Article 26 GDPR.
Determines the purposes and means of data processing. The final condition of controllership does not rely on the execution of data processing. The critical element is instead the position of the decision-making power.\textsuperscript{101} Even though the controller is permitted to decide the purpose of processing and its necessary components, the technical and organisational factors of data processing can in some aspects be delegated.\textsuperscript{102} A more detailed description would entail that the controller has the power of choice, and thus choose which data are to be processed, for what time, who shall be able to access the data, and what security measures have to be installed.\textsuperscript{103}

2.4.3 Processors
The GDPR also places data protection responsibilities on the processor. Similar to the definition of a controller, a processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf a controller.\textsuperscript{104} It can thus be concluded that a processor is brought to existence by the power of a decision by a controller.\textsuperscript{105} A processor is thus an external organisation to which the controller has delegated the entirety or parts of the data processing activities to.\textsuperscript{106} Two qualifications must be fulfilled to be regarded as a processor: (1) being a separate legal entity in relation to the controller; and (2) processing personal data on behalf of the controller.\textsuperscript{107}

2.4.4 Enforcement
The GDPR includes an arsenal of enforcement options for supervisory authorities,\textsuperscript{108} as well as including civil liability enforcement,\textsuperscript{109} both of which constitute an expansion in comparison to previous legislation.\textsuperscript{110} It was considered necessary to significantly increase fines, while at the same time also expanding the tasks and investigative powers of supervisory authorities to ensure effective personal data protection in the EU.\textsuperscript{111} In this essay the means of enforcement of supervisory authorities and by civil means, as well as the sanctions and fines, will not be discussed in any great detail. The focus of this essay lies in determining when the enforcement

\textsuperscript{101} Voigt & von dem Bussche, 2017, p. 19.
\textsuperscript{104} Article 4.8 GDPR.
\textsuperscript{105} Voigt & von dem Bussche, 2017, p. 20.
\textsuperscript{107} WP 169, 2010, p. 25.
\textsuperscript{108} Article 55.1, 56.1, 57.1, 58 GDPR.
\textsuperscript{109} Article 79, 82 GDPR.
\textsuperscript{110} See Article 28.1 Directive. See also Voigt & von dem Bussche, 2017, p. 201.
\textsuperscript{111} GDPR rec. 11. See also Voigt & von dem Bussche, 2017, p. 201.
capabilities are valid according to the provisions of the GDPR as well as by the territoriality principle in customary international law, e.g. when the GDPR is entitled to exercise jurisdiction. The severity of the battery of sanctions in the GDPR should not be understated. The maximum amount of fines have increased to € 20 000 000 000 or 4% of the total annual worldwide turnover,\footnote{Article 83.6 GDPR.} in conjunction with the risk of compensation claims from individual data subjects.\footnote{Article 82.1 GDPR.} Determining the jurisdictional scope of the GDPR is thus important from a compliance and liability aspect as private entities risk substantial economic loss.

### 2.5 The territorial scope of the GDPR

The territorial jurisdiction in the GDPR is not necessarily limited to EU member states.\footnote{Decision of 3/7/01 Case No. COMP/M2220 made pursuant to Article 8(3) of Regulation (EEC) No.4064/89 Merger Procedure (competition law); C-381/98 (commercial agents), see WP 56, p. 3-4.} The GDPR has been designed to provisionally widen the territorial scope of the Directive, which made indirect claims of extraterritorial jurisdiction.\footnote{See WP 56, p. 4, 6. See for instance the distance selling directive, where a consumer will not lose the protection granted by EU law by signing a contract containing a choice-of-law clause (Article 25).} Examining other areas of EU law,\footnote{For an early discussion on this matter, see WP 56.} it is obvious that the EU legislator considers EU law to have extraterritorial applicability when the issue at hand involves a ‘community dimension’ or a close link with the EU.\footnote{See WP 56, p. 4. See for instance the distance selling directive, where a consumer will not lose the protection granted by EU law by signing a contract containing a choice-of-law clause (Article 25).}

The GDPR is applicable to data subjects in the EU or to (online) behaviour taking place within the EU.\footnote{Svantesson, 2013, p. 92. This provoked major criticism when the Directive was adopted, see Cate, Fred H., 1995, and Bauchner, Joshua S., 2000, p. 715.} It might be interesting to clarify at what point in time the data subject must be situated in the EU for the GDPR to be applicable. According to some commenters, the decisive moment is when the data processing is performed. Using this line of thought, a temporary visitor to the USA would not fall under the jurisdiction of the GDPR during the period spent abroad. Other commenters argue that the time of the collection of the data is decisive, as that would fall in line with legislator’s idea of a comprehensive data protection regulation.\footnote{Decision of 3/7/01 Case No. COMP/M2220 made pursuant to Article 8(3) of Regulation (EEC) No.4064/89 Merger Procedure (competition law); C-381/98 (commercial agents), see WP 56, p. 3-4.}

The declared purpose for the creation of the GDPR was primarily to harmonize conditions in the internal market.\footnote{Voigt & von dem Bussche, 2017, p. 28-29.} Another reason was to prevent forum shopping amongst the member states to prevent unfair competition on the basis of differing rules on data protection.\footnote{C-131/12, Google Spain, rec. 54. See Voigt & von dem Bussche, 2017, p. 22.}
GDPR also provides an obstacle for forum shopping outside EU territory; the relocation to a third country does not evade EU data protection rules. Forum shopping might allow an entity to escape unsatisfactory law, and is not inherently malicious and ‘undesirable’. The significance of differing data protection law is also doubtful when forum shopping, as other factors – procedural costs, quality of bar, availability of evidence and the general legal conditions of the specific state – possibly are of greater importance in such cases. However, laws should prevent excessive or abusive forum shopping.

The introduction of the principle of lex loci solutionis enables jurisdiction over entities that are not located in EU-territory. The new forum principle means that applicable law, or jurisdiction, is dependent on where the associated contractual performance is executed. Generally the relevant location is where the contractual offer takes place. By offering their services to consumers or monitoring consumer behaviour, business organisations lacking establishment within the EU target data subjects in the EU which triggers the GDPR.

The territorial scope of the GDPR establishes several jurisdictional bases for identifying links to EU territory, and reads as follows:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

---

123 Svantesson, 2013, p. 74.
124 Svantesson, 2013, p. 73.
126 Svantesson, p. 75.
129 Article 3 GDPR. Article 3.3 GDPR is not aimed at general cases, but is meant be applicable to situations in which international law applies to ships or airplanes, or in situations related to diplomatic relations by international treaties, see rec. 25 GDPR. Also, see WP 179, p. 18.
The first provision takes aim at an entity’s activities as far as they can be linked to its establishment located on EU-territory, whether or not the conduct is executed within the EU. The second provision encompasses non-EU entities established outside EU-territory, and thus requires another type of link. In section 2.5.1 and 2.5.2 the links used in the GDPR will be examined, starting with the establishment-link in Article 3.1 which is followed by the links in Article 3.2 in sections 2.5.3 and 2.5.4.

2.5.1 In the context of activities of an EU establishment

The GDPR is applicable to processing of personal data in the context of activities of a controller or processor in the EU, even if the processing does not take place inside the EU. This is an application of the establishment principle, which determines the choice of law by the position of an entity’s establishment. Establishment presumes the effective and real exercise of activity through stable arrangements. Once again, the legislator stresses that the legal form is not the determining factor, whether it is through a branch or a subsidiary provided with its own legal personality. The place of formal legal actions, such as registration, does not equate place of establishment, but the place of registration provides an implication for the placement of the latter.

The broad definition was further widened in the Google Spain ruling, in which the Court stated that the term establishment must not be interpreted restrictively in order to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the right to privacy. A stable arrangement is determined by the nature of its economic activities and the services offered, and the two factors are to be evaluated in connection with each other. The size of the EU establishment is not the determining factor, it is the notion of stability. Even a single representative positioned inside a member state of the EU can be a sufficiently stable form of arrangement to constitute an establishment, if the representative offers services reliably on a continuous basis. Even possessing a bank account or a post office box inside the EU might be enough to be regarded as a stable arrangement.

---

131 GDPR, rec. 22.
132 GDPR, rec. 22.
133 C-230/14, Weltimmo, rec. 29.
134 C-131/12, Google Spain, rec. 53.
135 C-230/14, Weltimmo, rec. 29.
The presence of an establishment will have to be determined by the individual circumstances of each case.\textsuperscript{139} Additionally, stability is to be determined in connection to the particular nature of the activity. A business operation offering services exclusively over the Internet might thus qualify as an establishment if an arrangement associated with offering or administrating those services are present in a member state of the EU.\textsuperscript{140} It seems, however, that the threshold is quite low when it comes to businesses offering services exclusively online.\textsuperscript{141}

The extent of the activity’s contribution to the processing of data and the stability of the arrangements is also supposed to be measured. The economic activity inside the stable arrangement does not have to be of any great size – simply operating a website for offering services might suffice.\textsuperscript{142} In summary, both employees and equipment might qualify as stable arrangement.\textsuperscript{143} As long as the business organisation has an establishment in the EU, the GDPR extends to all its customers regardless of their nationality.\textsuperscript{144} Even if a non-EU controller does not have a presence inside a member state of the EU in the form of a subsidiary or a branch it does not mean it does not have an establishment within the meaning of EU data protection law.\textsuperscript{145} To summarise, the definition of an establishment on EU territory is extremely broad in the GDPR.

2.5.2 Data processing in the context of activities

Data processing only has to occur in the context of the activities of an establishment. The establishment of the controller or the processor does not have to execute any processing activities itself.\textsuperscript{146} In order for the GDPR to be applicable, it is sufficient that the EU establishment economically supports the data processing performed by the parent company. In the case of Google Spain, this was done by promoting and selling advertising space offered by a search engine which served to make the service offered by the search engine profitable.\textsuperscript{147} The crucial element is the connection between the economic activity of an establishment and

\begin{flushleft}
\textsuperscript{139} Voigt & von dem Bussche, 2017, p. 23.
\textsuperscript{140} Voigt & von dem Bussche, 2017, p. 23.
\textsuperscript{141} C-230/14 Weltimmo, recs. 29 and 31.
\textsuperscript{142} C-230/14, Weltimmo, recs. 31-33.
\textsuperscript{143} See Voigt; von dem Bussche, 2017, p. 23.
\textsuperscript{145} GDPR rec. 22. See EDPB, Guidelines 3, p. 4-5.
\textsuperscript{146} C-131/12, Google Spain, rec. 52. EDPB, Guidelines 3, 16-11-2018.
\textsuperscript{147} C-131/12, Google Spain, rec. 55.
\end{flushleft}
the performance of data processing.\footnote{C-131/12, \textit{Google Spain}, rec. 52.} The territorial location of the data processing is not the decisive factor under this provision – it may be within or outside EU-territory.\footnote{EDPB, Guidelines 3, p. 4-5. See Voigt \& von dem Bussche, 2017, p. 24.}

The territorial location is thus important to determine the place of establishment of the controller or the processor and any business presence of a non-EU controller or processor. Territorial location is not important for determining the location of the data processing or the location of the data subjects. The physical location of the data is not the decisive factor; the location of the entities, controllers and processors, is the important location to determine for direct or voluntary application.\footnote{WP 179, p. 8. See EDPB, Guidelines 3, p. 8.}

\subsection*{2.5.3 Targeting data subjects in the EU}

Data processing activities related to the offering of goods or services, irrespective of whether a payment of the data subject is required falls under the territorial scope of the GDPR.\footnote{Article 3.2a GDPR.} This provision will primarily impact business organisations operating on a multinational level offering services through the Internet.\footnote{Voigt \& von dem Bussche, 2017, p. 26.} To determine if goods or services are aimed at data subjects in the EU, it should be confirmed if the controller or processor specifically envisions offering goods or services inside the EU.\footnote{GDPR rec. 23.} An intention on the side of the business organisation to address EU consumers must be verified.\footnote{Voigt \& von dem Bussche, 2017, p. 26.} Website accessibility, email addresses or other contact details are deemed as insufficient to show this. Similarly, using the general language of the third country in which the business organisation is established is also insufficient to show intention, e.g. a US business organisation might not address individuals in the United Kingdom because of the use of the English language on their company website.\footnote{GDPR rec. 23. See Voigt; von dem Bussche, 2017, p. 26.} Nevertheless, examples of indicators for targeting individuals in the internal market are the usage of a language generally spoken in a EU member state; accepting payment in currencies originating in a member state (in particular the Euro); or alluding to European customers or users; or offering delivery to a member state: or the domain name of the website relates to a member state (e.g. xxx.com/se).\footnote{Cases C-585/08 and C-144/09, \textit{Pammer and Hotel Alpenhof}, recs. 80-84. GDPR rec. 23. See also Voigt \& von dem Bussche, 2017, p. 26.} This list is not exhaustive. It may be expanded at will and include more
contrived examples for determining if targeting has occurred. In addition to being targeted in this fashion, data subjects can also be targeted through the monitoring of their behaviour.

2.5.4 Monitoring data subject behaviour

Data processing that takes the shape of monitoring of EU customer’s behaviour falls under the territorial scope of the GDPR. In order to determine if monitoring have taken place, it should be established if EU individuals are tracked on the Internet. That includes potential future use of personal data processing methods in which individuals are profiled, especially when processing is undertaken in order to take decisions concerning an individual or for analysing or predicting an individual’s personal preferences, behaviours and attitudes. In brief, any form of web tracking is considered monitoring. Common web tracking techniques are e.g. cookies and certain social media plug-ins. The key condition, profiling, can take many different shapes and be performed through a variety of tools. Even without using infamous cookies, web browsers transfer an array of data when accessing a website to the website provider to ensure that the website is displayed in an optimal way. This generates a browser fingerprint, which in combination with other sources of information such as IP addresses, enables the provider to identify users whenever they access the website.

2.6 Data transfers to third countries

Cross-border data transfers are vitally important to multinational business organisations, and are frequently made between EU and non-EU entities. Such transfers will commonly involve transferring data to a third country, meaning a State that is not a member state of the European Union. Due to the complexity of ensuring an adequate level of data protection in the cross-border transfer situations the GDPR has numerous provisions to provide a high level of security. Any transfer of personal data that is undergoing processing or is intended for processing after transfer to a third country or international organisation has to comply with the relevant provisions in the GDPR. The legislation also includes provisions for onward transfers of

---

157 Article 3.2b GDPR.
158 GDPR rec. 24.
160 Ibid.
161 Ibid.
162 Since 2018-07-20 members of the European Economic Area (Iceland, Liechtenstein and Norway) are incorporated into the GDPR. For more information, see [http://www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576]. Accessed 2018-11-29.
163 The relevant provisions are Articles 44-50 GDPR, Article 44 GDPR. See also, Voigt & von dem Bussche, 2017, p. 117.
personal data from the third country or international organisation to a different party, to ensure that such onward transfers upholds the high level of protection the GDPR demands.\footnote{164

Non-EU entities operating in third countries lacking adequate protection are given contractual means of adequacy. This is made possible by providing non-EU entities with self-regulatory instruments which forcibly incorporates GDPR provisions in contractual clauses or agreements. Through these voluntary compliance agreements provided for in the GDPR, the EU legislator is able to distribute EU data protection rules and standards through the discretion of business entities operating internationally. The voluntary compliance agreements consist of Standard Contractual Clauses (SCC), Binding Corporate Rules (BCR) and Codes of conduct and certification. The transfer of personal data pertaining to an EU individual are only possible if the third country provides similar data protection standards to EU law.\footnote{165
Kuner, 2017, p. 893. See C-362/14, Schrems, recs. 45.}
The transfer of personal data to a third country therefore constitutes the link to apply EU data protection law indirectly.\footnote{166
See Kuner, 2013, p. 125 et seq. Also Kuner, 2017, p. 893.}
This can be viewed as an aspect of the so called ‘Brussels effect’, whereby the EU unilaterally influences regulation through its central position in global commerce.\footnote{167
See Bradford, 2012.}
EU rules on data transfers have meant that many third countries has adopted similar data protection legislation to maintain access to the EU market for entities within their territory.\footnote{168

\subsection*{2.6.1 The trouble with consent}

Transfers of personal data to a third country are allowed to be executed even if the third country cannot guarantee adequate data protection if the data subject has explicitly consented to the transfer proposal.\footnote{169
Article 49.1a GDPR. See also Voigt & von dem Bussche, 2017, p. 119.}
This is in accord with the right of privacy of individuals, a central theme in current EU data protection law that entitles individuals to decide on the use of their personal data.\footnote{170
Article 6.1a, 7.1 GDPR.}
To ensure validity the consent has to explicitly relate to the proposed data transfer where consent given implicitly or in general are not considered sufficient.\footnote{171
Article 49.1a, 61a GDPR. See also Voigt & von dem Bussche, 2017, p. 118.}
As the data subject has to be informed about the potential risks related to the data transfer,\footnote{172
Voigt & von dem Bussche, 2016, Art. 49, rec. 2. See also Voigt & von dem Bussche, 2017, p. 118.}
etlies to convey that the data subject’s personal data will not be shielded by the same level of data protection as in the GDPR.\footnote{173
Voigt & von dem Bussche, 2016, Art. 49, rec. 2. See also Voigt & von dem Bussche, 2017, p. 118.}
however not fully understood.\textsuperscript{174} Outside of the requirement for \textit{acquiring} consent, data subjects are entitled to withdraw consent at any given time.\textsuperscript{175} Using consent as a legal basis for data transfers to third countries is consequently not recommended.\textsuperscript{176}

### 2.6.2 Adequacy decisions

In the GDPR, a transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors in that third country (or the international organisation) in question ensures an adequate level of protection.\textsuperscript{177} Factors to be assessed when determining if a third country provides an adequate level of protection includes the third country’s rule of law, data protection regulation, implementation, supervision, respect for human rights, procedural law and international commitments.\textsuperscript{178} Judging by the wording of the relevant provision in the GDPR, equal or complete compliance with all of the criteria are not required; the adequate level of protection is determined by an overall assessment of the specific circumstances.\textsuperscript{179} However, examining relevant case law yields other results.\textsuperscript{180} If a third country wishes to allow entities within its territory to do business with the EU market, the State will have to legislate EU-conformant data protection laws that are in essence equivalent to EU data protection standards.\textsuperscript{181} Data transfers made by entities situated in third countries may be executed without prior authorisation.\textsuperscript{182} The use of adequacy decisions can be viewed as a function of the ‘Brussels effect’, by which the EU uses its economic influence to exercise unilateral regulation of global commerce.\textsuperscript{183} In the context of data protection, the Brussels effect is displayed through the influence of EU law on the data protection regulation is many countries outside the EU.\textsuperscript{184} Through adequacy decisions EU spreads its data protection regulation to global trading partners.\textsuperscript{185} The EU is able to use its economic clout to project EU data protection law globally.

\begin{itemize}
\item \textsuperscript{174} Voigt & von dem Bussche, 2016, Art. 49, rec. 2.
\item \textsuperscript{175} Article 7.3 GDPR. See also Voigt & von dem Bussche, 2017, p. 97, 119.
\item \textsuperscript{176} Voigt & von dem Bussche, 2017, p. 119.
\item \textsuperscript{177} Article 45.2 GDPR.
\item \textsuperscript{178} Article 45.2a GDPR. See also Voigt & von dem Bussche, 2017, p. 117.
\item \textsuperscript{179} Article 45.1 GDPR. See also Voigt & von dem Bussche, 2017, p. 117.
\item \textsuperscript{180} Primarily the C-326/14, \textit{Schrems}.
\item \textsuperscript{181} C-362/14, \textit{Schrems}, recs. 73 and 74. See Kuner, 2017, p. 893.
\item \textsuperscript{182} See GDPR rec. 103.
\item \textsuperscript{183} Bradford, 2012. Exemplifying the Brussels effect in data protection, see p. 22. See also Birnhack, p. 513.
\item \textsuperscript{184} See Greenleaf, 2012, for instance p. 74. Also Bygrave, 2014, p. 53-54.
\end{itemize}
2.6.3 EU – U.S. Privacy Shield

Globally the U.S.A. is the world’s largest receiver of data and consequently a strong supporter of abolishing restrictive laws on international data transfers. The U.S. State and U.S. private entities are, not surprisingly, not the biggest fans of the comprehensive, wide-reaching EU data protection law, the GDPR being its current iteration. The U.S. and EU has for long had different data protection regulation, in the sense that the very structure of the legislation is different. While EU data protection law is comprehensive and establishes rules for both public and private entities which are enforced by supervisory authorities, U.S. data protection law is limited to public entities and select sectors that are considered sensitive. The private sector, however, is largely self-regulated, where companies are allowed to formulate their own corporate privacy policies. U.S. businesses, used to making their own privacy policies are naturally rustled by the comparatively stringent data protection standards of EU law, affecting business operations and considerably increasing the cost of compliance. With the strengthening of enforcement in the GDPR, the impact this would have on U.S. multinational business groups was severely criticised as the liability for U.S. tech companies would increase considerably. Nonetheless, U.S. businesses has voluntarily complied with EU data protection standards by changing privacy policies to conform to EU data protection legislation. U.S. businesses has also voluntarily entered the Safe Harbor, now known as the Privacy Shield, which forces U.S. businesses operating in the EU internal market to comply with EU data protection regulation even when data are processed on U.S. territory.

Regarded as a controversial adequacy decision under the Directive, the EU-U.S. Privacy Shield enables U.S. entities to be certified as adequate third country parties. The Privacy Shield has continued to function under the GDPR, as adequacy decisions made under the

---

187 Stewart, 2000, p. 1887. See Cate, Fred H., 1995, p. 432 (regarding the draft Directive), criticizing its comprehensiveness. Also, see Shaffer, 2000, p. 8, where the author argues that EU data protection legislation not only threatens U.S. State sovereignty, but also the sovereignty of private business decisions. See also Kuner, 2010, p. 177. U.S. law also makes extraterritorial claims in its data protection legislation, recently amending the Stored Communications Act by passing the Clarifying Lawful Overseas Use or Data (CLOUD) Act, extending the territoriality of U.S.-based entities to any data stored outside U.S. territory in the name of crime prevention, see H.R. 4943, section 2-3 in particular.
188 Bradford, 2012, p. 23
190 Shaffer, 2000, p. 75.
previous legislation has continued to function.\textsuperscript{195} The Privacy Shield is the successor of the Safe Harbor adequacy decision of 2000, which was declared invalid by the Court of Justice in the Maximilian Schrems-case.\textsuperscript{196} The Safe Harbor framework was criticised by the ECJ primarily because of lacking any verdict on U.S. rules on limiting interference with fundamental rights of individuals and rules of effective legal protection.\textsuperscript{197} For instance, personal data cannot be protected against U.S. agencies once it is located on U.S. servers.\textsuperscript{198} A response to this might be to store personal data on territory-specific servers.\textsuperscript{199} The Privacy Shield is an instrument separated from the GDPR – it targets data transfers outward-bound from the EU, and thus U.S. business organisations operating within EU territory may well be impacted by provisions in the GDPR, their cooperation with the Privacy Shield framework notwithstanding.\textsuperscript{200}

In practice, amongst U.S. business organisations EU data protection law has had a Brussels effect, in that it has been an important factor in how U.S. businesses have shaped their processing of personal data,\textsuperscript{201} as multinational companies have defaulted to the ‘highest common denominator’,\textsuperscript{202} whereby it is understood that the most comprehensive data protection rules are prescribed by the EU. Thus, (U.S.) businesses operating globally reduces their compliance costs by complying with the most demanding regulatory framework, as separating non-EU data from EU data is also difficult,\textsuperscript{203} or at least very costly.\textsuperscript{204} Consequently, for many U.S. multinational business groups it is simply easier to treat all data as if it originated in the EU.\textsuperscript{205}

Through their own economic might in the areas of technology that relate to data treatment, U.S. sovereignty can challenge the EU, which has resulted in the special treatment of the U.S. through the Safe Harbor and the Privacy Shield. The interconnectedness of the two economies should also not be understated; the compromise with regards to transfers of personal data to the U.S. might have been a small price to pay for continued trans-Atlantic trade.

\textsuperscript{195} Article 45 GDPR.
\textsuperscript{196} C-362/14, Schrems. Incidentally, the Schrems-case can be interpreted as another illustration of the ‘Brussels effect’, see Padova, 2016, p. 145.
\textsuperscript{197} C-362/14, Schrems, recs. 88-89.
\textsuperscript{198} See C-362/13, Schrems.
\textsuperscript{199} This is known as data localisation, see Greenleaf, 2017, p. 197-198.
\textsuperscript{200} Czerniawski, 2017, p. 238.
\textsuperscript{201} Birnhack, 2008, p. 512, 515, 517-518.
\textsuperscript{202} Bamberger & Mulligan, 2011, p. 269-270.
\textsuperscript{203} Bradford, 2012, p. 25.
2.6.4 Standard Contractual Clauses

Business organisations operating in third countries whose legislation does not provide an adequate level of data protection in relation to the GDPR may use EU Standard Contractual Clauses (SCC). This gives business organisations the ‘option’ to formulate private law contracts in which the data protection requirements of the GDPR are incorporated into the contract itself. SCC were a frequently used solution under the Directive for data transfers to and from third countries. The usage of an SSC only guarantees an adequate level of data privacy protection for the data importer in the third country, not for the entire third country. Under the SCC-provisions, if the data transfers fulfils the relevant conditions it is regarded as a destination of adequate data protection. The clauses of an SCC cannot be altered, as the entire standard contract must be complete for the provision to be valid. The SCC that was formulated in accordance with the Directive is still valid until amended, replaced or repealed. So far, there are three SCC has been adopted by the European Commission: two contracts for data transfers from controllers situated inside the EU to controllers outside the EU, and one contract for data transfers from controllers inside the EU to processors outside the EU. It will have to be seen if the SCC will be altered in the future, as there have been some doubts about the adequacy levels the contracts will achieve under the GDPR. In terms of jurisdiction, the contracts bind the third country controller or processor to the EU-based controller, locking the non-EU entity to the law of the EU member state of the data exporter, with enforceability

---

206 Article 46.2 c-d GDPR. Pending authorisation of the competent supervisory authority, adequate data protection safeguards can also be provided by contractual clauses, see Article 46.3 a GDPR. The SCC are provided by the European Commission and thus have a wider range of application compared to individual contracts approved by supervisory authorities, see Voigt; von dem Bussche, 2017, p. 119.


209 Article 44 GDPR.

210 Voigt; von dem Bussche, 2017, p. 120.

211 Article 46.5 GDPR.


213 Available at the same website as shown in the note above.


belonging not only to the parties of the contract but also to data subjects.\textsuperscript{216} Liability under SCC are joint and thus shared between the data exporter and data importer,\textsuperscript{217} which causes strong motives for the data exporter to demand that the third country data importer adheres stringently to EU data protection standards.

Through SCC the EU projects its data protection standards through the contractual relationships of private entities. The advantages of SCC are many. SCC are ready-made clauses compliant with the GDPR, and does not have any limitations concerning the relations between the contracting parties. Furthermore, it can used where more than two parties are involved.\textsuperscript{218} Disadvantages of SCC are primarily the lack of individuality and flexibility, as the contract has to be adopted unaltered and completely. Furthermore, concerning intra-group processing the contracts has to be individually adopted between the separate group members, which makes using SCC very arduous for multinational business groups who exchange data on a daily basis.\textsuperscript{219} In this case, Binding Corporate Rules provides an alternative.

\section*{2.6.5 Binding Corporate Rules}

For business groups established within the EU and operating in third countries lacking adequate data protection regulation, an additional alternative to an adequacy decision are self-regulation in the shape of Binding Corporate Rules (BCR).\textsuperscript{220} BCR is a legal instrument invented by the Article 29 Working Party in order to allow multinational business groups to integrate EU data protection provisions into their corporate privacy policy,\textsuperscript{221} thus forming a shell of adequate protection relating to their business group specific data processing requirements.\textsuperscript{222} Contrary to the Directive, the GDPR introduces detailed requirements concerning the contents of BCR.\textsuperscript{223} Valid BCR are legally binding and apply to and are enforced by every member of a business group, or a collaboration of business organisations engaging in joint economic activity.\textsuperscript{224} BCR are both internally and externally binding, binding every business within the group and third

\textsuperscript{216} Decision 2001/497/EC, rec. 16-17; Decision 2004/915/EC, Annex Set II, III (a); Decision 2010/87/EU, rec 19, 22.
\textsuperscript{217} Decision 2001/497/EC, clause 6(2). See Bond et al., 2002, p. 189. The joint liability is lessened in Decision 2004/915/EC, see clause III (a); and in Decision 2010 2010/87/EU, see rec. 20. In both contracts the parties are only responsible for liability as far as the extent of their contribution to the breach.
\textsuperscript{218} Voigt & von dem Bussche, 2017, p. 122.
\textsuperscript{219} Moerel, 2012, p. 90.
\textsuperscript{220} See WP 256, 257.
\textsuperscript{221} See Moerel, 2012, p. 91.
\textsuperscript{222} Voigt & von dem Bussche, 2017, p. 125.
\textsuperscript{223} Article 26.2 Directive and Article 47 GDPR. This also means that different types of data cannot be treated differently, such as having separate standards for employee and customer data, see GDPR rec. 48 and Moerel, 2012, p. 106. See also Voigt & von dem Bussche, 2017, p. 125.
\textsuperscript{224} Article 47.1a GDPR.
party entities respectively. Data transfers in a BCR-relationship between a controller established in the EU to other controllers or processors established in a third country within the same group have, so called BCR-Controllers (BCR-C), have a different definition compared to BCR-Processors (BCR-P). BCR-P apply to data transfers from a non-group controller established in the EU that are processed by group members as processors. Thus, BCR-C apply to intra-group data processing relations, whereas BCR-P apply to group members including outside of the EU acting as a processor under the instructions of non-group EU-based controller.

In terms of jurisdiction, the liability for breach of a BCR-C belongs to the controller or processor established on the territory of an EU member state or the EU-member designated to accept delegated data protection responsibility for liability, except if the EU-entity proves that it is not responsible for the misconduct. Concerning BCR-P, the BCR-member is responsible for all liabilities and does not have the option to demonstrate that a non-EU member was responsible. In the context of BCR-members in third countries, BCR-C must also contain clauses conferring jurisdiction on to EU authorities if a non-EU member violates the BCR. In the case of BCR-C, this is another example of bypassing the strict territoriality in enforcement jurisdiction – by binding several entities to a BCR, business groups or collaborations are locked to EU data protection standards by the means of an EU group member. A ‘softer’ version of this is applied in BCR-P, as the jurisdiction does not by contractual design fall under EU authority, but means that EU data protection rules governs the data transfer relationship between EU and non-EU entities all the same. This has the effect of turning the BCR into the privacy policy of the business organisation, as per the accountability principle. As shown, BCR is a potent way of transforming the privacy policies of multinational companies into instruments of EU data protection law.

225 Article 47.2c GDPR. See Moerel, 2012, p. 23.
226 WP, 256, p. 2. See also Moerel, 2012, p. 105 et seq.
227 WP 256, p. 2; WP 257, p. 2.
228 WP 256, p. 2. WP 257, p. 2.
229 WP 256, p. 2.
230 WP 257, p. 2.
231 WP 256, p. 8.
232 Article 47.2f GDPR in connection with Article 82.2-5 GDPR.
233 WP 257, p. 9.
234 WP 256, p. 8.
235 See WP 154, p. 3. Also, see Moerel, 2012, p. 100-101.
236 Article 5.2 GDPR. See also WP 256, p. 3. See Moerel, 2012, p. 178.
2.6.6 Codes of Conduct and Certification

To extend the compliance with the GDPR, self-regulation procedures are expected to play a more important role in future data protection law. Codes of conduct and Certification mechanisms are self-regulation instruments provided as options in the GDPR, and ensures an adequate level of data protection and can thus constitute a legal basis for third country data transfers. Non-EU entities are able to comply with an approved Code of conduct with general validity in order to ensure they have appropriate safeguards for importing data from the EU. The non-EU entities must in addition make commitments that are binding and enforceable, via contractual or other legally binding instruments in order to apply those safeguards. Concerning Certification mechanisms, non-EU entities can also acquire a certification that demonstrates the existence of an appropriate level of data protection. The certificate can function as a justification for international data transfers if, similarly to Codes of conduct, the importing entity makes commitments that are binding and enforceable to apply the safeguards.

2.6.7 Derogations for particular situations

Even if adequate, or as we have witnessed, essentially equivalent data protection standards are lacking, data transfers to third countries can in limited situations still be performed. Furthermore, the list of derogations is exhaustive. Data transfers using a derogation as a legal basis are permissible if the transfer is necessary for a contract with the data subject, the transfer is necessary for a contract with a third party, the transfer is necessary for important reasons of public interest, the transfer is necessary for the protection of vital interests, or for the prevailing legitimate interests of the controller. The derogations are limited in scope

---

238 Article 40, 41 GDPR.
239 Article 42, 43 GDPR.
240 Article 46.2e-f GDPR.
241 Article 40.3 GDPR, see Article 46.2e GDPR.
242 Article 40.3 GDPR. See also Voigt & von dem Bussche, 2017, p. 130.
243 Article 42.2 GDPR, see Article 46.2f GDPR. Also, see Voigt & von dem Bussche, 2017, p. 130.
244 Article 42.2 GDPR. See also Voigt & von dem Bussche, 2017, p. 130.
246 Article 49.1.1 GDPR. See WP 114, 2005, p. 13 et seq.
247 Article 49.1c GDPR.
248 Article 49.1d GDPR.
249 Article 49.1f GDPR.
250 Article 49.1-2 GDPR. Using this derogation, the transfer cannot be repetitive, must be limited in scope and still has to be shielded by suitable safeguards. Furthermore the legitimate interests of the controller can be outweighed by the rights of data subjects, more in Voigt & von dem Bussche, 2017, p. 132-133.
and thus multinational groups should not and cannot rely on them for providing a legal basis.\textsuperscript{252} The appropriate procedure is therefore to use them rarely, and comply with the GDPR, conforming data protection standards with EU data protection law.

\subsection{2.6.8 Representatives of non-EU entities}

Entities that fall under the territorial scope of the GDPR but situated outside the EU have to appoint a representative in the EU.\textsuperscript{253} This encompasses every controller or processor offering data subjects in the EU goods or services or monitoring their behaviour,\textsuperscript{254} unless they fulfil the conditions for exemption.\textsuperscript{255} For entities that are not public authorities or bodies, all three conditions in 27.2a GDPR has to be met: the processing is (1) occasional; (2) does not include special categories of personal data (Article 9.1 GDPR) or personal data relating to criminal convictions and offences; and (3) that is unlikely to result in a risk to the rights and freedoms of natural persons.\textsuperscript{256} This is supposed to supply supervisory authorities and data subjects with a point of contact within the EU.\textsuperscript{257} Most importantly the appointment of a representative does not affect the liability or responsibility of the entity – controller or processor – with regards to the processing activities.\textsuperscript{258}

\subsection{2.7 Brief summary}

It can be concluded that the jurisdictional provision in the GDPR makes very broad claims. Besides entities that are established on EU-territory, the territorial scope of the GDPR latches on to non-EU entities that target or monitor EU data subjects. Proceeding to third country data transfers, non-EU States are able to acquire an adequacy decision that affirm that the level of data protection in that State is essentially equivalent to that of the EU. Entities cannot rely on data subject’s consent and derogations as legal bases for operating in non-EU States that lack an adequacy decision. Consequently, the available legal bases are adequacy decisions and the voluntary compliance agreements (SCC, BCR and Codes of conduct/certification). The conclusions shown here indicates that the EU legislator, by virtue of the GDPR, seeks to regulate the conduct of entities that in fact fall under the territorial jurisdiction of other States. The relations between sovereignty, jurisdiction and territory will be explored in the next section.

\begin{enumerate}
\item Voigt & von dem Bussche, 2017, p. 133.
\item Article 27 GDPR. See further EDPB Guidelines 3, p. 19 et seq.
\item Article 3.2a-b GDPR.
\item Article 27.2 GDPR.
\item Article 27.2 a GDPR.
\item Article 27.5 GDPR; GDPR rec. 80. See also Voigt & von dem Bussche, 2017, p. 133.
\end{enumerate}
3 Sovereignty, jurisdiction and territory in data protection

Sovereignty and jurisdiction are terms that has not been used with much precision. They have both been used to describe the entirety of a State’s exclusive control of its territory and the legal order the State chooses to impose. Some distinction can be ascertained, as authors has found some regularity in the meaning of the terms: Sovereignty refers to complete, supreme and exclusive authority over a physical space, its people, and its laws. Jurisdiction can be derived from sovereignty, and is a term generally used to describe the limits of legal competence of a State or other legal authorities, to make, apply and enforce rules of conduct on individuals.

3.1 Sovereignty and territory

Conventional theories of sovereignty and jurisdiction centre on the notion of territory. The application of law regulating cross-border data shares the same fundamental qualification, that a transfer of data must have crossed territorial borders, and thus moved from one sovereign jurisdiction to another. To accurately fulfil this qualification, it is essential to determine when a particular set of personal data have crossed territorial borders, and therefore to determine a data set’s location at a given point in time.

Defining territories to which sovereignty can be had, and jurisdiction may be exercised in, is not obvious concerning data processing. ‘Internet’ mostly refers to the public and commercial Internet, which is not the exclusive avenue for data processing, even though it is very widely used. ‘Cyberspace’ is a broader, but also consequently a fuzzier term which is important to define by virtue of its intended use, which is to say ‘with an understanding of the processes taking place in the computerized world’ and their interaction with international law, e.g. the principles governing sovereignty and jurisdiction. For instance, ‘processing’ in the

259 Svantesson, 2013, p. 65.
262 Tsagourias, 2015, p. 17.
266 Kuner, 2013, p. 122.
267 Ibid.
268 Tabansky, 2011, p. 77.
269 The public Internet is used by approximately 48 % of the total world population, whereas in developed countries the figure is 81 % [https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf] retrieved 2019-01-03.
270 Tabansky, 2011, p. 76.
sense of EU law encompasses basically everything that relates to any treatment of data. Thus, a general definition of cyberspace has to equally be able to fit every facet of data use within its meaning, and not just the specific cyberspace of the public Internet or the ‘enclosed cyberspace’ a company’s intranet. Cyberspace can be described as having three layers. The first layer consists of the physical space of computers, integrated circuits, cables and other equipment and infrastructure; the second layer consists of the software logic; and the third layer consists of data and electronics.

Cyberspace can be subject to sovereignty. Seemingly borderless actions taken in cyberspace can be regulated locally by a sovereign State. Sovereignty can be construed as the basic constitutional framework of international law and was built around principles and rules establishing formal equality among States by awarding each State sovereignty. Sovereignty is closely linked with territory and has been a successful concept for organising territory effectively. Data cannot exist freely; it requires software to interpret, but most importantly it requires equipment in which it can stored. The popular view is that data transferred through the Internet (cloud data) are continuously moving, making it inconceivable to specify in which State the data are located at any point in time. This is false. As a technical fact, the data has to be stored on a physical device, one which is located in a facility which is obviously located in a specific State. In the majority of cases, data are copied or duplicated across a range of separate data centres to guarantee continuity and backup for business purposes. In most cases it is possible to establish at which data centre the fragments of a set of personal data are stored, or even pinpoint the specific piece of equipment. Nonetheless, it can still difficult to determine when an activity occurred; when data was transferred or processed.

Furthermore, the parties responsible for the equipment and the execution of the data processing exist in the physical space, e.g. within a territory. Cyberspace cannot exist without

---

271 See section 2.3 (Processing).
272 Tsagourias, 2015, p. 15; Kuehl, 2009, p. 28.
273 Tabinsky, 2011, p. 77-78.
274 Tsagourias, 2015, p. 22.
275 Tsagourias, 2015, p. 16.
280 Kuan Hon; Millard, 2012, p. 32.
281 Ibid.
282 Stewart, 2000, p. 1826.
283 Tsagourias, 2015, p. 24. See Stewart, 2000, p. 1826. Contrary to this essay, the authors makes the assumption that activities in cyberspace are impossible to posit to a physical territory.
being anchored in the physical space and is worthless without physical people using it, and both of these are located inside the territory of a Sovereign state.

4 Types of jurisdiction

In the context of cyberspace, jurisdictional issues all face the same central question: which laws do entities have to adhere to in relation to their online activity, or in this case, their data processing activities. From a State perspective, which State has the privilege to regulate which activity?

In the judgement of the Lotus case the court made the significant distinction between prescriptive and enforcement jurisdiction. In international legal scholarship, jurisdictional bases are commonly divided into three categories, although with considerable overlap. The jurisdictional bases interacts with the principles, e.g. the reach of a jurisdictional base is only as long as a certain jurisdictional principle allows it to be, and the reach of a jurisdictional principle is only as long as the permissiveness of the relevant link.

This prompts an important question of the distinction between prescriptive and enforcement jurisdiction. What is the point of prescribing rules if there is no way to enforce them? Aside from the fact that there might be valid reasons why a State might want to take a clear stance on a particular issue, the noncompliance by a person affected by the extraterritorial prescription may cause severe consequences. The person could receive a fine; assets could be seized; the person could be stopped from entering the territory. Thus, in situations where there exists reciprocal interests between States, extraterritorial compliance is possible. Where there are no overlapping interests, extraterritorial prescriptive jurisdiction is generally not successful.

---

286 See Kohl, 2015, p. 35.
290 See Elche, 2013, p. 60.
291 See Kohl, 2015, p. 36. Svantesson, 2013, p. 68-69. Svantesson calls this ‘bark’ and ‘bite’ jurisdiction, in that prescriptive jurisdiction without enforcement jurisdiction is not as useless as it might seem at first glance. Compare Bygrave, 2000, p. 255. Bygrave calls this ‘regulatory overreaching’.
293 Ibid.
4.1 Prescriptive and adjudicative jurisdiction

Prescriptive jurisdiction is the power of a state to apply its laws to cases involving a foreign component, or a specific subject matter.\(^{294}\) Adjudicative jurisdiction is the power of the courts of a State to hear cases involving a foreign element – to adjudicate a certain subject matter.\(^{295}\) As already established in the methodology-section, it is doubtful that adjudicative jurisdiction is necessary to single out in relation to EU data protection law, as the prescriptive situation will lead to the same result – applicable law is determined by jurisdiction.\(^{296}\)

Prescriptive jurisdiction under customary international law has its starting point in the judgement of the Permanent Court of International Justice (PCIJ) in the Lotus case of 1927. From the judgement it can be ascertained that the approach of prescriptive jurisdiction is that ‘everything that is not prohibited is permitted’.\(^{297}\) In the jurisdictional context, this makes the principles of prescriptive jurisdiction – territoriality and nationality – permissive bases and the single definite restrictive rule is the non-interference rule concerning enforcement jurisdiction.\(^{298}\) In the context of cross-border activities and extraterritorial regulatory reach, the principles of prescriptive jurisdiction are scarcely restrictive. They do, however, imply that a link between the regulation and the activity that the State seeks to regulate is required, as without any restrictions on the exercise of jurisdiction the jurisdictional principles would be unnecessary.\(^{299}\) However, the low requirements means that the bar for identifying such links have almost no limits, as States will likely seek to regulate activities they have an interest in, something they have a connection to.\(^{300}\) Prescriptive jurisdiction is thus permissive of extraterritorial claims, as long there is some link connecting the claim to interests of the State.

4.2 Enforcement jurisdiction

Enforcement jurisdiction is the ability of a state to carry out acts within the territory of another state.\(^{301}\) If this was to be executed extraterritorially this would truly encroach upon the other State’s sovereignty. In the context of EU data privacy law, a hypothetical example could include an EU data privacy supervisory authority’s conduct outside the EU.\(^{302}\) Enforcement jurisdiction

---


\(^{298}\) Kohl, 2015, p. 37.

\(^{299}\) Ibid.

\(^{300}\) Ibid.


in customary international law is limited to the territoriality principle.\textsuperscript{303} The strict territoriality of enforcement jurisdiction ‘(…) is a rock solid pillar of international law.’\textsuperscript{304} It means that even though States have extended their provisional regulatory reach to entities inside other territories, it might struggle to enforce this de facto extraterritorial regulation. Thus, extraterritorial enforcement jurisdiction can only be exercised with permission of the State which inhabits the territory on which the related entity is located in.\textsuperscript{305}

There are ways to overcome the strict territoriality of enforcement jurisdiction. One possible solution is to provide entities with voluntary compliance possibilities. ‘Voluntary’ is used in the widest sense of the word, as without the ‘voluntary’ compliance the online entities will not obtain access to a certain State. This can be achieved either by opening localised entities in the relevant territories, or by forcing ‘voluntary’ contracts upon entities wanting access to the territory in question.\textsuperscript{306} Together with the option of supervisory authorities to ban controllers and processors from processing data, this could be likened with drawing territorial borders in cyberspace.\textsuperscript{307}

5 Jurisdictional bases

There are two general approaches to applying jurisdiction in public international law. The expansive approach allows States to exercise jurisdiction freely unless there is a prohibitive rule that hinders it.\textsuperscript{308} The restrictive approach prohibits free exercise of jurisdiction unless there is a permissive rule that allows it.\textsuperscript{309} The restrictive approach has been used by most States and is the approach most widely reflected in doctrine and is thus supposedly reflects customary international law.\textsuperscript{310} Both approaches to jurisdictional delimits are founded on State sovereignty;\textsuperscript{311} the expansive approach gives States the sovereign entitlement to unilaterally exercise jurisdiction, whereas the restrictive approach highlights the reciprocity of the international legal order – by asserting its own sovereignty, a State also recognizes the sovereignty of other States.\textsuperscript{312}

\textsuperscript{304} The Case of the SS Lotus, 18a. Kohl, 2015, p. 51.
\textsuperscript{305} Lowe & Staker, 2010, p. 335. See Kohl, 2015, p. 51.
\textsuperscript{306} Kohl, 2015, p. 51 and 49.
\textsuperscript{307} See Kohl, 2015, p. 52.
\textsuperscript{308} This approach was taken by the Court in the Case of the SS Lotus, see Ryngaert, 2008, p. 21.
\textsuperscript{310} Ryngaert, 2008, p. 21.
\textsuperscript{311} Ryngaert, 2008, p. 29.
Under the restrictive approach States are not allowed to exercise jurisdiction unless they can depend on a permissive principle, such as the territoriality principle.\(^{313}\) The general opinion seems to favour the restrictive approach, which restricts States to exercising jurisdiction where there is a permissive principle.\(^{314}\) This also seems to be in line with the supposed purpose of international law of jurisdiction: ‘delimiting States’ spheres of action and thus reducing conflicts between States.’\(^{315}\) In order to justify legitimate State interest which may not fit perfectly within the definition of a permissive principle, the principles are very broad.\(^{316}\) Consequently, States are usually allowed to exercise jurisdiction if there is a legitimate interest based on a territorial or personal link of the subject matter.\(^{317}\) The extent of a State’s discretion is thus quite broad, as the connections required to exercise jurisdiction can be construed in a number of ways.\(^{318}\) This has resulted in many cases of concurrent jurisdiction.\(^{319}\)

The permissive principles approach is thus the main framework for determining legitimate exercise of jurisdiction.\(^{320}\) The Harvard Research Draft Convention on Jurisdiction with Respect to Crime (Harvard Draft) has been especially important in the popularity in this approach.\(^{321}\) The Draft was a research project, and sought to identify the jurisdictional grounds that States depended on with reference to criminal jurisdiction.\(^{322}\) The Harvard Draft identifies five general jurisdictional principles: the territoriality principle; the nationality principle; the protective principle; the universality principle; and the passive personality principle. Nevertheless the Harvard Draft never made it into a treaty, which consigns the jurisdictional scope of States to customary international law, with the associated issues of determining what the law is at any point in time.\(^{323}\)

The permissive principles approach typically links sovereignty with territoriality, and thus considers territorial jurisdiction the fundamental rule of international jurisdiction.\(^{324}\) The supremacy of territoriality is based on the sovereign equality of States and the principle of non-interference,\(^{325}\) which renders legislation that has the effect of regulating conduct of foreigners

\(^{313}\) Ryngaert, 2008, p. 21.
\(^{314}\) Ibid.
\(^{315}\) Buxbaum, 2006, p. 304. See also Ryngaert, 2008, p. 21, and Mann, 1984, p. 30 et seq.
\(^{316}\) Ryngaert, 2008, p. 21-22.
\(^{317}\) Ryngaert, 2008, p. 22.
\(^{318}\) Ibid.
\(^{319}\) Ibid.
\(^{320}\) Ryngaert, 2008, p. 28.
\(^{322}\) Svantesson, 2013, p. 134.
\(^{324}\) Island of Palmas arbitral case, p. 829. See Ryngaert, 2008, p. 28.
\(^{325}\) Ryngaert, 2008, p. 29. See Elche, 2013, p. 60.
in foreign States unlawful.\footnote{Mann, 1984, p. 47. See Ryngaert, 2008, p. 29.} An attribute shared amongst the permissive principles of jurisdiction is the required link between State competence and governing the subject matter.\footnote{Ibid.} This link is not always the territory in the physical space, but also encompasses connections relating to the population of the State or its sovereign authority.\footnote{Ryngaert, 2008, p. 31.} In short, a State is not permitted to exercise jurisdiction unless it has a legitimate interest in the activity, or when it is not affected by the activity in question.\footnote{Ibid.}

The territoriality principle is important in data protection law.\footnote{Ryngaert, 2008, p. 31.} The territorial scope of the GDPR requires links that closely resemble a variant of the objective territoriality principle: the targeting destination approach (targeting principle).

### 5.1 Territoriality principle

The international legal order consists of States with sovereign power over its territory and has exclusive jurisdiction within that territory,\footnote{Coughlan et al., p. 4. Lowe & Staker, 2010, p. 313.} which is why the territoriality principle remains the most basic jurisdictional principle.\footnote{Ryngaert, 2008, p. 21, 42.} In a domestic context, territorial jurisdiction indicates a State’s capacity to exert power of individuals, places and things through legislature, courts and executive within the sovereign territory of the State.\footnote{Coughlan et al., p. 4.} In an international context it relates to the capacity of a State to exert the same power extraterritorially (beyond its own territory). Exerting power extraterritorially attracts the interest of other states whose territory the extraterritorial jurisdiction implies an infringement of.\footnote{See Coughlan et al., 4.} A State’s jurisdiction over activities and actors inside its sovereign territory is connected through the territoriality principle.\footnote{Lowe & Staker, 2010, p. 320. Hillier, 1998, p. 254.} Through the principle, the State is allowed to prescribe and enforce laws within its territory. The territoriality principle thus applies to conduct that is contained within one State’s territory.\footnote{Hillier, 1998, p. 254.} As shown in section 2, the establishment principle in the GDPR uses an attachment to EU-territory as the link justifying the EU’s jurisdiction over the relevant activities. Some acts which affect a State’s territory was either initiated in another State, or was initiated in the first State but only had effects inside another State. To resolve such situations, the territoriality
principle may be complemented by two variants: the subjective territoriality principle and the objective territoriality principle.\textsuperscript{337}

5.1.1 Subjective territoriality principle

This is the term given to the exercise of jurisdiction over conduct that was initiated inside the State’s territory, but was realized within another State’s territory.\textsuperscript{338} In the context of cyberspace, the application of subjective territoriality would make forum shopping very easy, as it would be very easy to find a suitable jurisdiction in which to perform online activities from, as the data would still be projected worldwide.\textsuperscript{339} Muir-Watt eloquently describes the starting point: ‘there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it.’\textsuperscript{340} Thus, the application of the subjective territoriality principle in the context of cross-border online activities would undermine national values and rights.\textsuperscript{341} This is consequently not the route chosen for the GDPR.

5.1.2 Objective territoriality principle, effects principle and passive personality principle

First a note on the similarity between the objective territoriality principle and the effects principle.\textsuperscript{342} It seems as if the only element distinguishing one from the other is that the effects principle does not appear to have a specific requirement that the effects must be a consistent element of the misconduct in question. However it is most likely easily established and can be presented if the conduct is suitably framed.\textsuperscript{343} The principles both hone in on the effects an action has on a certain State’s territory,\textsuperscript{344} where the objective territoriality principle is based on conduct that is initiated outside the State but realized inside the State;\textsuperscript{345} similarly, the effects principle is based on conduct performed outside the State but that has effects inside the State.\textsuperscript{346}

\textsuperscript{337} Lowe & Staker, 2010, p. 320-321.
\textsuperscript{339} Schultz, 2008, p. 811.
\textsuperscript{340} Muir-Watt, 2003, p. 695.
\textsuperscript{341} See Schultz, 2008, p. 811. See also Goldsmith & Wu, 2005, p. 110 et seq.
\textsuperscript{342} Compare Svantesson, 2013, p. 136-139.
\textsuperscript{343} See Kohl, 2015, p. 47-48, note 81.
\textsuperscript{344} Lowe; Staker, 2010, p. 321-323.
Jurisdiction may be exercised when an activity has effects inside a State’s territorial borders. The effects principle stems from the Lotus case and is an accepted jurisdictional base in many areas of law. However, there are differing views on the scope of the effects principle and the extent of the effects required to trigger a State’s jurisdiction; should the effects already have been felt; the substantiality of the effects; the degree of damage caused; and if predictable effects are to be included. This is the principle chosen as the link for Article 3.2 GDPR, in order to prevent the evasion described by Muir Watt in the section above. The GDPR uses a qualified version of the objective territoriality principle, which is the targeting principle. This qualification will be examined in the following section.

5.1.3 The targeting principle
An issue with jurisdiction concerning online activity is that the activities might have been felt in several different territories, which creates concurrent jurisdiction. The link many States have placed great reliance on is a territorial connection between the online activity and the State, where a for example a website can be accessed from the territory of a State, even though the servers are located in territory elsewhere. This is known as the accessibility destination approach, and has been used in prominent cases on territorial application of laws on online activities. The link used in the GDPR is another version of the destination approach, known as the targeting principle. The targeting principle has been developed to allow States to exercise jurisdiction regardless of effects perceived in other jurisdictions, if the territory of the State is targeted by the online activity. Targeting can be described as a notion that is greater than mere effects, but lesser than a physical presence. According to this version of the destination approach every State is not justified to regulate online activity just because it is accessible from the State; only those States who are specifically targeted by the online activity or actor has the privilege to regulate it.

347 Kohl, 2015, p. 20.
348 Tsagourias, 2015, p. 20. Arrest Warrant, para. 47.
349 Tsagourias, 2015, p. 20. See U.S. v Yousef, p. 112.
350 Tsagourias, 2015, p. 20.
351 See Kohl, 2015, p. 38.
352 Kohl, 2015, p. 38.
354 Article 3.2 GDPR in connection with Kohl, 2015, p. 44.
357 C-131/12 Google Spain, rec. 56. See Kohl, 2015, p. 45.
The destination approaches can be seen as aspects of the objective territoriality principle or the effects principle. In customary international law cross-border misconduct, the State whose geographical position is located on the territory in which the foreign misconduct is committed has the right to regulate the activity: the objective territoriality principle, or effects principle. This is joined by the State where the misconduct originated; this is known as the subjective territoriality principle. Thus the subjective territoriality principle has concurrent rights of jurisdiction together with the objective territoriality principle; the origin versus destination. The key to the understanding this lies in the effects the foreign act has on the State’s territory. The impact of the effects provides the fundament for subjecting the foreign actor to another State’s laws. The impact does have to be physical in nature, and can include the impact of economic activities as well as other intangible effects.

The targeting principle can be seen as a qualification of the objective territoriality principle and the effects principle, as it means that the activity initiated outside the State must have been intended to have effects on the territory of the State. The benefits in using the targeting principle are manifold: it (1) reduces the number of concurrent jurisdictions, as the number of targeted States ought to be lower than the number of affected States; it also (2) presents a more predictable jurisdictional model, as online entities are only subject to the laws of States they intended to send the information to; it also (3) raise the threshold of the required link between activity and the effects on a State; and (4) it also makes forum shopping unviable as it would prove pointless for entities to move to more lenient jurisdictions while still targeting the same territory.

However, the targeting principle is not faultless. In comparison with the subjective territoriality principle (the location of the activity) and the objective territoriality/effects principle it is difficult to determine what targeting implies. The global nature of the Internet implies that targeting is by default made worldwide. The decisions taken by the entities might, however, determine the threshold of what constitutes targeting: the language used on the website; the default currency of the website; user consent of using the website from a certain

---

358 Kohl, 2015, p. 47.
359 The Case of the SS Lotus, No. 19. See Kohl, 2015, p. 48.
360 See Kohl, 2015, p. 50.
361 Kohl, 2015, p. 48.
362 Ibid.
364 Geist, 2001, p. 1404.
territory are just a few examples.\textsuperscript{368} The delimitations of the targeting principle are thus vague, and might well mean whatever the regulatory authority decides.\textsuperscript{369} The targeting provision in the territorial scope of the GDPR uses the given examples and more in order to determine if EU data subjects was targeted. The fact that the physical equipment used to execute the conduct is placed on a territory in which the conduct is accepted is not a valid argument in the real world, and similarly in cyberspace.\textsuperscript{370} The application of extraterritorial jurisdiction on the basis of conduct targeted at a particular territory does not seem exorbitant as the conduct in question was intended to have an effect in one territory alone, e.g. only targeting data subjects in the EU.

The requirement consists of a link between the party and the territory that does not necessarily exist in the physical space.\textsuperscript{371} As shown in section 3.1, data does exist in the physical space, in the sense that data are stored on equipment placed within physical and territorial borders. According to the targeting principle, the physical presence of the personal data stored for processing purposes is not required, as is the case with the targeting-provision in the GDPR. Through cyberspace, foreign entities located in one territory are able to form relations with individuals located in another territory without physical contact ever taking place.\textsuperscript{372} Individuals within a territory can thus be targeted by entities located outside it, often for economic reasons.\textsuperscript{373} The element enabling extraterritorial jurisdiction consists of the link that invokes the objective territoriality principle or effects principle: the effect the targeting of individuals has within the territory the authority seeks to regulate.\textsuperscript{374}

5.2 Other permissive principles

\textit{Personality and nationality principle}. Jurisdiction can be exercised on the basis of the State of nationality of either the perpetrator (active personality or nationality) or the victim (passive personality).\textsuperscript{375} The personality principle is primarily used in criminal law.

The scope of the GDPR is focused on data subjects in the EU. It is tempting to apply one of the personality principles to the GDPR provisions. However, as it is focused on data subjects in the

\textsuperscript{368} See Schultz, 2008, p. 818.
\textsuperscript{369} Ibid.
\textsuperscript{371} Stewart, 2000, p. 1827.
\textsuperscript{372} Ibid.
\textsuperscript{373} Ibid.
\textsuperscript{374} See Geist, 2001, p. 1380. Also, see Henn, 2003, p. 163.
\textsuperscript{375} Ryngaert, 2008, p. 88, 96. Kuner, 2010, p. 188. See Lowe & Staker, 2010, p. 323. The passive personality principle is strongly contested even in the context of criminal jurisdiction. Consequently the required link between State interest and misconduct is particularly demanding. In addition, the passive personality principle was not listed in the Harvard Draft, see further Hillier, 1998, p. 279 and Lowe & Staker, 2010, p. 330.
EU, a territorial approach is taken. Furthermore it does not specify that the data subjects has to be nationals or residents of an EU member state (even though they naturally often are); it is the territorial confines that matter.

It could be argued, however, that the liability stipulated in the SCC, BCR and Codes of Conduct is a variant of the accountability principle, which means that the EU-entity is responsible for the data when transferred to a non-EU entity. This bases the liability, and thus jurisdiction, on the EU-nationality of the controller or processor situated in the EU.

It has been commented that the territorial scope of the GDPR referring to the Monitoring of behaviour-provision exercises jurisdiction on the basis of the passive personality principle.\textsuperscript{376} However, it seems more apt to place monitoring into the same category as consumer targeting, as monitoring also targets the personal data of data subjects in the EU.

**Protective principle.** Jurisdiction can be exercised on the basis of the protection of a State from conduct committed in another territory that jeopardize its sovereignty.\textsuperscript{377} This principle is mostly limited to criminal law and acts that endanger State security.\textsuperscript{378} Furthermore the protective principle is focused on the protection of the State and not the protection of individuals. The jurisdictional scope stipulated in the GDPR protects data subjects, and not individual States.\textsuperscript{379}

**Universality principle.** Jurisdiction exercised on the basis of the universal principle mostly refers to the most severe crimes.\textsuperscript{380} Jurisdiction based on this principle is often based on the expansive approach developed in Lotus; as shown above, in practice the opposite of Lotus is often true (the restrictive approach).\textsuperscript{381} Formally the GDPR does not make the claim to have the right to regulate across the globe. However, it might be possible to view the territorial scope of the GDPR as having global effects, infringing on the sovereignty of other States.

Having ruled out the other permissive principles (apart from the aspects in which they can be said to expose themselves indirectly) the territoriality principle remains, and will thus the focus of the continuing analysis.

\textsuperscript{379} Article 3 GDPR.
\textsuperscript{380} Lowe & Staker, 2010, p. 326.
\textsuperscript{381} Ryngaert, 2008, p. 27
6 Analysis

Before proceeding with the analysis, a brief recollection of the findings in the previous section: The GDPR exercises jurisdiction on the basis of the territoriality principle, connecting entities to EU data protection law by virtue of the establishment principle and the targeting principle. Prescriptive jurisdiction can be exercised extraterritorially, whereas enforcement jurisdiction is strictly territorial. The practical examples given at the start of the essay will be revisited. Relating the analysis to the examples shows how this plays out in a practical sense, contrasted to the very theoretical framework which has been discussed thus far.

Example A

*Company X is a multinational company with its main office in a third country. Company X has subsidiaries situated in several member states of the European Union. Company X transfers personal data from the European Union to its main office in the third country regularly.*

Company X has establishments in several member states of the EU. The GDPR is applicable according to the establishment principle, which enables prescriptive and enforcement jurisdiction. To smoothen business operations a voluntary compliance agreement would be recommended to make sure that all group members follow EU data protection standards.

Example B

*Company X is situated inside a member state of the European Union. Company Z is situated inside a third country. Company X transfers personal data for processing purposes to Company Z, which Company Z subsequently transfers back to Company X.*

The GDPR is applicable to Company X by the establishment principle, and is thus under prescriptive and enforcement jurisdiction. By the accountability principle, Company X is responsible for the personal data they transfer to Company Z. This transfer requires a legal basis, which will most likely result in Company Z entering a voluntary compliance agreement, barring Company Z is situated inside a third country with an essentially equivalent standard of data protection. The controller in this situation is Company X. Lacking an adequacy decision a voluntary compliance agreement is required. As the EU-entities are processors, this puts considerable responsibility on the non-EU controller by virtue of the accountability principle.
The liability is shared between the data exporter and the data importer, which most likely means that the EU-processors will want to be wholly certain of Company X’s privacy policy.

**Example C**

*Company X and Company Z are both situated inside a third country. Company X has several customers in EU member states and collects personal data on individuals inside member states of the EU. Company X transfers data to Company Z for processing purposes.*

The GDPR is applicable to Company X by virtue of the targeting principle, thus extending prescriptive jurisdiction. However, it is doubtful if enforcement jurisdiction is achievable. Company Z is processing personal data gathered from EU data subjects, and is in extension hit by the GDPR. Theoretically, barring the existence of an adequacy decision, if Company X wants to continue offering services or monitoring customers to EU data subjects, it will have to abide by EU data protection rules. If Company Z wants to continue doing business with Company X, they will most likely have to enter a voluntary compliance agreement with Company X. Two entities outside the EU, in their dealings with each other must in this scenario still abide by data protection standards set by the EU and not their territorial sovereign.

6.1 **The prescriptive and enforcement jurisdiction of the GDPR**

According to the territorial scope in the GDPR, the EU may exercise jurisdiction on the basis of connecting factors that relate to the territoriality principle; (1) the establishment principle and (2) the targeting principle. Aspects of the remaining permissive principles can be discerned in the territorial scope of the GDPR, but does in fact only relate to the aspects they share with the territoriality principle. The establishment principle relate to the ‘full’ territoriality principle and to some extent the subjective territoriality principle, as it focuses on entities that are located within EU-territory. The targeting principle relate to the objective territoriality principle, or the effects principle, as it targets entities that are located outside EU-territory. These principles will be analysed in relation to prescriptive and enforcement jurisdiction.

Beginning with prescriptive jurisdiction, data transfers constitute a particular obstacle in preventing unfavourable conduct, in that it is a medium that crosses borders very easily. The objective territoriality principle constitutes a link that seem acceptable in customary international law. By exploiting the EU market through targeting or monitoring data subjects, non-EU entities bind themselves to the data protection standards of the EU. The use of the objective territoriality principle can create an abundance of concurrent jurisdictions. The GDPR
uses a qualified version, wherein the conduct originating outside the EU but is realized within
the EU has to be targeted at data subjects in the EU. This qualified version is known as the
targeting principle, which may reduce the number of concurrent jurisdictions and may also
provide entities with a degree of legal foreseeability. The intent of the entity is the deciding
factor, judged according to a list of examples that signify the intent of targeting data subjects in
certain territories. Developments to the list of examples will be interesting to observe, as it will
most likely be extended as far the ECJ requires it to.

What is the importance of the location of data in relation to the territoriality principles?
Data transfers take place in cyberspace. Cyberspace is not a unique location void of territory,
but very much exists in the physical space through the equipment giving it its existence and the
people giving it its purpose. Enforcement jurisdiction can as previously shown only use the
‘full’ territoriality principle as a jurisdictional base, which would mean that the data storage
equipment and entities would have to be located within EU-territory. The GDPR does not base
its jurisdiction on the basis of the location of the physical equipment holding the data, but the
intent of the entity. Consequently, the physical containment of data outside the EU does not
affect the territorial scope of the GDPR.

The extraterritorial dimension of the GDPR might look like it bites off more than it can
chew. Regarding concurrent jurisdiction it seems more apt to identify the GDPR as regulatory
overreaching. But it is not without its purpose – if entities worldwide want to have access to the
EU market they have to adhere to EU data protection laws. However, regulatory overreaching
is distinguished by the unenforceability of the concerned regulation. In that respect the GDPR
might be overreaching, as the territoriality principle may prohibit certain enforcement activities.
Nonetheless, potentially overreaching prescriptive jurisdiction is not without its merits. The EU
legislator has identified a lack of data privacy protections worldwide and have decided to take
a clear stance on this particular issue, thus constructing the GDPR to be extraterritorial in order
to protect individuals in the EU by upholding the human rights treaties it is party to. And in
cyberspace, any such regulation must be extraterritorial.

It is clear that prescriptive jurisdiction provides for an openness in jurisdictional terms,
whereas enforcement jurisdiction can only be strictly based on full territoriality. The EU
legislator has provided the GDPR with ways of bypassing the strict territoriality of enforcement
jurisdiction by extending the broad allowance of prescriptive jurisdiction through different legal
means. This method of bypassing consists of voluntary actions by States and private entities.
However, these actions are not purely voluntary – the prescriptive jurisdiction of the GDPR
excludes entities that do not comply with the GDPR from the EU-market.
6.2 Extending prescriptive jurisdiction

Only within the physical borders of a State’s sovereign jurisdiction is the State able to enforce its prescriptions. In the case of the GDPR, the EU legislator has provided means of escaping the strict territoriality of enforcement jurisdiction, or if following the terminology established in the previous part, ‘improper’ jurisdiction. This could be expressed as extending prescriptive jurisdiction by nudging foreign States and private entities. The accountability principle also creates a heavy burden for controllers in relation to their data processing, establishing responsibility and liability for all processing initiated by them, and in relation to third country data transfers, comes with a responsibility for the non-EU controller or processor. This makes EU-entities an extension of the EU legislator, in that the EU-entities have an obligation to make sure that any non-EU entities they engage with complies with EU data protection standards. The potency of the voluntary jurisdiction is thus a result of an externality which the theories on jurisdiction has not really accounted for, as EU data protection law is boosted by the EU’s central position in the global economy, in what is known as the Brussels effect.

One way of spreading EU data protection law is using the adequacy decision. These decisions on the level of data protection of a third country provides the European Commission with a tool to dictate the data protection standards of States outside the EU. The extraterritorial reach of the GDPR may be perceived as an infringement on the sovereignty of other States. Not only the economic power of the EU-market makes this possible, but the overall comprehensiveness of EU data protection regulation. Entities in non-EU States that have adequate levels of data protection are not formally under the jurisdiction of the EU. However, it could be argued that they are de facto covered by the prescriptive jurisdiction of EU data protection law, as the prescriptions have essentially been copied by the non-EU State, in a kind of legislative transfer. The power to exercise jurisdiction over entities and conduct within the territories of non-EU States are removed from the territorial sovereigns, and becomes subject to legislation adopted by people they did not elect.

The U.S. in particular views this as an encroachment on the U.S. State, but also as a major obstacle for doing business. The U.S. can by its position as a global economic powerhouse still determine which rules impact them. It is nevertheless clear that even if the U.S.A. is reluctant to legislate similar data protection regulation as the EU, private entities in the U.S. have been relatively quick to comply with the ‘highest common denominator’. The perceived infringement of State sovereignty have thus been bypassed by pushing private entities into voluntary agreements.
Non-EU entities operating in third countries lacking adequate protection are given other means of ensuring adequacy. This is made possible by providing non-EU entities with contractual instruments which forcibly incorporates GDPR provisions to private contracts. The many separate business entities that together form the economic power of the EU are forced to use a voluntary compliance tool in order to do business internationally. Thus the territorial scope in the GDPR, acceptable according to prescriptive jurisdiction, but rejected in enforcement jurisdiction, is given enforcement by contractual instruments.

As for the individual voluntary compliance options, SCC provides tools to extend EU data protection law by incorporating GDPR-provisions into contracts between entities. Through SCC the EU projects its data protection standards through the contractual relationships of private entities. In the case of BCR, this is another example of bypassing the strict territoriality in enforcement jurisdiction – by binding several entities to a BCR, business groups or collaborations are locked to EU data protection standards by the means of an EU group member. The final ‘voluntary’ compliance tool are the Codes of conduct and certificates, which are developed to basically take the form of a privacy policy, and is thus a form of self-regulation. Nevertheless, entities using these tools have to bind themselves through legal means, which in this case means a contract that can be enforced.

Recurring in all the voluntary solutions is the accountability principle and the joint liability. The accountability principle means that controllers and processors are responsible for data they have transferred out of their direct management. This responsibility is related to the liability. Using the establishment principle, the responsibility and liability is placed at the EU-entity, who has to prove that they were not responsible for any breach. The entity is located within EU-territory, and is thus enveloped in both prescriptive and enforcement jurisdiction. The situation is different under the targeting principle. If the entity is not located within the EU, only prescriptive jurisdiction can be exercised. Through voluntary compliance tools the strict territoriality of enforcement jurisdiction can be bypassed. An EU-based controller working with a processor based in a third country will thus carry the liability for any breach of the data protection standards stipulated in the GDPR. This creates enormous incentives for controllers to ensure that their collaborators abide by EU data protection rules.

The EU legislator has viewed it a necessity to make sure that the GDPR guarantees the rights bestowed on data subjects in the EU. This has resulted in a comprehensive legislation with a broad scope of application. Consequently the jurisdictional scope of the GDPR is very wide to prevent forum shopping. To guarantee the rights of the data subjects and the free flow of data, the width of the GDPR’s jurisdiction has to cover all data that contains identifiers.
belonging to data subjects in the EU – as soon as data contains identifiers on EU data subjects, the GDPR is applicable.

The economic clout of the EU means that the prescriptive jurisdiction of the EU is very potent and can make any entity that wishes to operate in the EU market to comply with EU data protection standards. The duality of prescriptive and enforcement jurisdiction does not factor for the externality that economic power brings, and the advantage that comes from regulating a cross-border phenomena first, or at least, most comprehensively. This has resulted in creating something that could be called ‘market-force jurisdiction’. It could be argued that this is simply an inescapable facet of the international legal order, whereby States exhibiting greater power in economy or military and so on will always have power to push other States toward their legislative concepts and standards, nibbling at the borders of their sovereignty. Even though the means giving life to cyberspace exist in the physical space, cyberspace might exacerbate this as territorial borders are easily crossed. The significance of a State’s physical territory is diminished, and is instead attached to the regulatory authority of a State, which in the case of the EU, is amplified by its economic power. In an environment that is inherently transborder, exclusion from one the most lucrative territories is a severe consequence. Thus, the prescriptive jurisdiction together with the externality of the EU economy provides a voluntary enforcement vehicle for applying the GDPR worldwide – the prescriptive jurisdiction is extended through voluntary means.
Table of References

**Bibliography**

Akehurst, Michael, Jurisdiction in International Law, in *British Yearbook of International Law*, vol. 46, p. 145, 1972-73.


Bennett, Colin J.; Raab, Charles D., Revisiting the governance of privacy: Contemporary policy instruments in global perspective, in *Regulation and Governance*, 2018.


Czerniawski, Michał, Extraterritoriality in the Age of the Equipment-Based Society: Do We Need the ‘Use of Equipment’ as a Factor for the Territorial Applicability of the EU Data Protection Regime?, in Svantesson, Dan Jerker B.; Kloza, Dariusz (eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, 2017, Intersentia.


Esteve, Asunción, The business of personal data: Google, Facebook, and privacy issues in the EU and the USA, in International Data Privacy Law, vol. 7, p. 36-47, 2017.


González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, Springer.


Kuan Hon, W; Millard, Christopher, *Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA? (The Cloud of Unknowing, Part 4)*, Queen Mary University of London, School of Law, 2012.


World Economic Forum et al., *Personal Data: The Emergence of a New Asset Class*, 2011.


**Table of Cases**

**European Court of Justice**


Case C-369/98, The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher, European Court Reports 2000 I-06751.

Joined Cases C-465/00, C-138-01 and C-139/01 Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer Rundfunk, European Court Reports 2003 I-04989.

Case 101/01, Criminal Proceedings against Bodil Lindqvist, 6 November 2003, European Court Reports 2003 I-12971.


Joined Cases C-585/08, Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alphenhof GesmbH v Oliver Heller, European Court Reports I-12527.

Case C-366/10, Air Transport Association of America and Others, 21 December 2011, European Court Reports 2011 -00000.

Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014, ECLI:EU:C:2014:317.

Case C-362/14, Maximilian Schrems v. Data Protection Commissioner, 6 October 2015, ECLI:EU:C:2015:650.

**European Court of Human Rights**


S. and Marper v. the United Kingdom (30562/04) and (30566/4), judgment of 4 December 2008.

**International Court of Justice and Permanent Court of International Justice**


**Other**


**Table of Authorities**
Convention for the protection of individuals with regard to automatic processing of personal data, CoE, European Treaty series No. 108, 1981.

**Reports and other documents**

**European Union**
COM (1990) 314 Final. Commission communication on the protection of individuals in relation to the processing of personal data in the community and information security.
Commission Decision of 03/07/2001 declaring a concentration to be incompatible with the common market and the EEA Agreement, Case No COMP/M.2220 – General Electric/Honeywell, OJ L48/1, 2004.


Information on adequacy decisions:

Information on the EU – U.S. Privacy Shield:

Information on SCC:

**European Data Protection Board (Article 29 Working Party)**

Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56.


Working Document Setting up a framework or the structure of Binding Corporate Rules, 1271-00-01/08/EN, WP 154.


Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, 176/16/EN, WP 176.

Opinion 1/2010 on the concepts of “controller” and “processor”, 00264/10/EN, WP 169.

Opinion 8/2010 on applicable law, 0836-02/10/EN, WP 179.

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN, WP 238.
Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (updated), 17/EN, WP 256.
Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (updated), 17/EN, WP 257.

**Miscellaneous**


International Telecommunications Union
Accessed 2019-01-03.