Department of Law
Spring Term 2017
Master’s Thesis in Private International Law and EU Law, following an Internship at the Hague Conference on Private International Law
30 ECTS

Cross-Border Application of EU’s General Data Protection Regulation (GDPR)
– A private international law study on third state implications

Tillämpning av EU:s dataskyddsförordning över landgränserna
– En internationellt privaträttslig studie om tredjestats implikationer

Author: Anni-Maria Taka
Supervisor:
Professor Maarit Jänterä-Jareborg
Contents

Abbreviations .................................................................................................................. 5

1 Introduction .................................................................................................................. 7
  1.1 Background ............................................................................................................. 7
    1.1.1 EU’s answer to cross-border data flows ......................................................... 7
    1.1.2 Internship at the Hague Conference on Private International Law ........... 9
  1.2 Objective of the study ........................................................................................... 10
  1.3 Delimitations ......................................................................................................... 12
  1.4 Method and sources ............................................................................................. 14
  1.5 Outline .................................................................................................................. 19

2 EU data protection law ............................................................................................... 21
  2.1 The fundamental right to data protection and its legal basis ............................... 21
    2.1.1 Article 16 of the TFEU and Article 8 of the Charter ....................................... 21
    2.1.2 Data protection and privacy – two separate rights ......................................... 22
    2.1.3 A fundamental right – but not an absolute right ........................................... 23
    2.1.4 Is there a fundamental right to data protection in horizontal situations? ...... 23
  2.2 An historic overview of the data protection legislation in Europe ....................... 25
    2.2.1 Developments since the 1970s .................................................................... 25
    2.2.2 The Data Protection Directive (DPD) .............................................................. 26
  2.3 The GDPR and its new criteria ............................................................................. 29
    2.3.1 The GDPR provides new aspects to EU data protection law ....................... 29
    2.3.2 Who is covered by the GDPR? .................................................................... 30

3 Data subjects in the EU ............................................................................................. 32
  3.1 Natural persons enjoying the protection of the GDPR ...................................... 32
    3.1.1 Who is a data subject according to the GDPR? ............................................ 32
    3.1.2 The significance of nationality and residence ............................................... 35
    3.1.3 Data subjects physically present in the EU ................................................... 36

4 Establishment and its implications .......................................................................... 38
  4.1 Controllers and processors .................................................................................. 38
  4.2 Establishment as a key concept .......................................................................... 39
    4.2.1 Google Spain and Google ............................................................................. 41
    4.2.2 Weltimmo ..................................................................................................... 43
  4.3 Which cross-border situations are covered by the GDPR? ................................. 45
5 Offering goods or services to data subjects in the EU .................................................. 47
  5.1 Identifying the criteria in Article 3(2)(a) of the GDPR ...................................... 47
    5.1.1 Offer of goods or services ................................................................. 48
    5.1.2 The concept of targeting .................................................................... 48
  5.2 The concept of targeting and EU case law ...................................................... 50
    5.2.1 Targeting and consumer contracts ...................................................... 51
    5.2.2 Targeting in the field of intellectual property rights .............................. 56
  5.3 Interpretation of Article 3(2)(a) in the light of EU case law ......................... 59
    5.3.1 The targeting approach and effet utile .................................................. 59
    5.3.2 Accessibility of a website – not a sufficient factor ................................. 60
    5.3.3 Intention to target .............................................................................. 61
    5.3.4 Targeting the entire world .................................................................. 65
  5.4 Data subject in a contractual relationship ....................................................... 66
    5.4.1 Data subjects as consumers ................................................................. 66
    5.4.2 The GDPR in relation to the Rome I Regulation ..................................... 68
  6 Monitoring the behaviour of data subjects in the EU ......................................... 72
    6.1 The notion of monitoring ......................................................................... 72
    6.2 Online tracking of data subjects ............................................................... 73
    6.3 Processing of personal data ...................................................................... 76
    6.4 The broad notion of monitoring ............................................................... 78
    6.5 Behaviour that takes place in the EU ......................................................... 81
    6.6 Is an intention to monitor required? ......................................................... 82
    6.7 Cross-border situations that fall outside the territorial scope of the GDPR .... 84
  7 Conclusions ..................................................................................................... 87
Sources .................................................................................................................. 93
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charter</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>CJEU (or ‘the Court’)</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>Convention 108</td>
<td>Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, 28 January 1981</td>
</tr>
<tr>
<td>Council</td>
<td>Council of the European Union</td>
</tr>
<tr>
<td>ECHR</td>
<td>Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR (or ‘Regulation’)</td>
<td>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)</td>
</tr>
<tr>
<td>HCCH</td>
<td>Hague Conference on Private International Law</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SvJT</td>
<td>Svensk Juristtidning</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union (Consolidated version) of 26 October 2012</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union (Consolidated version) of 26 October 2012</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>29WP</td>
<td>Article 29 Data Protection Working Party: Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The Working Party has, under Article 29 of the Directive 95/46/EC (‘DPD’), an advisory status and acts independently (See Articles 29 and 30 of the DPD, and recital 65 of the DPD). The Working Party is composed of national supervisory authorities, a representative of the EU institutions and bodies, and a representative of the European Commission (See Article 29(2) of the DPD).</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background

1.1.1 EU’s answer to cross-border data flows

“In a modern state it is normally understood that, in the absence of special indications widening or narrowing the class, its general laws extend to all persons within its territorial boundaries.”¹

The internet has challenged the important position of the territoriality principle in private international law.² Thus, the internet has not changed the fact that the world is, as it has been for thousands of years now, divided by geographical borders that separate different state territories. Nevertheless, the internet is often considered as being borderless since it is not limited by geographical borders. E-mails are sent from one state to another without border checks, and data freely crosses national borders between most states.³ Data flows are constantly crossing these borders “as easily as the air we breathe”.⁴

An individual living in the European Union (‘EU’) visits a website of a company located in the United States of America (‘US’). This company uses cookies on its website and in that way tracks its visitors, including this individual. An interesting question is which law is the applicable law to the processing of personal data in this particular situation? To know which law is to be applied is highly important since the regulation concerning the processing of personal data can vary significantly in different countries around the world. The increased cross-border data flows also raise questions about how to regulate these cross-border situations on an international level.

Notably, there is at present no international treaty on the applicable law and international jurisdiction regarding processing of personal data. Despite the issue’s global nature, there are no binding international standards for international data transfers. However, solutions

---

² Svantesson, D, Private International Law and the Internet, p 8-9.
³ Svantesson, D, Private International Law and the Internet, p 56-57.
⁴ Reding, V, Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world, Speech of the Vice President of the European Commission, p 4.
can be found on a regional level.\textsuperscript{5} For example, the EU provides rules that regulate the territorial scope of EU data protection law when the data controller is established outside the EU. Article 4 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (‘DPD’) has been described as constituting the first set of rules in an international data protection instrument to deal specifically with the determination of applicable law.\textsuperscript{6} In May 2018, the DPD will be replaced by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (‘GDPR’).\textsuperscript{7}

One of the most significant changes in the GDPR compared to the DPD is its territorial scope when the controller or the processor is not established in the EU.\textsuperscript{8} The GDPR extends the application of EU data protection law far beyond the borders of the EU.\textsuperscript{9} When the controller or the processor has no establishment in the EU, the GDPR will apply to the processing of personal data of data subjects who are in the EU, where the processing activities are related to the offering of goods or services to the data subjects in the EU, or to the monitoring of the behaviour of those data subjects.

This highly current and interesting issue of the applicability of the GDPR in cross-border situations is the topic of this study. Surprisingly, this topic has received rather limited attention amongst academics, and is therefore ripe for scholarly examination.

\textsuperscript{5} Spiecker genannt Döhmann, I, The European Approach towards Data Protection in a Globalized World of Data Transfer, in: Dörr, D, Weaver, R, Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries, p 61.
\textsuperscript{6} Bygrave, L, Determining Applicable Law pursuant to European Data Protection Legislation, p 1.
\textsuperscript{7} According to Article 99(2) of the GDPR, the Regulation shall apply from 25 May 2018.
\textsuperscript{8} Article 3(2) of the GDPR can be considered to be “one of the more important ‘achievements’ of the reform”, see De Hert, P, Czerniawski, M, Expanding the EU data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.
\textsuperscript{9} See De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 230 ff.
1.1.2 Internship at the Hague Conference on Private International Law

During the first 12 weeks of the master’s thesis course I completed an internship at the Hague Conference on Private International Law (‘HCCH’), in The Hague, the Netherlands. The internship at the HCCH was an extremely valuable experience. I had the opportunity to experience what it is like to work in an important international organisation in the field of private international law. During my internship I carried out legal research, both in English and French, on particular issues of private international law and comparative law. My tasks consisted, in particular, of carrying out legal research and legal translation work in relation to the February 2017 draft Convention on the Recognition and Enforcement of Foreign Judgments, the drafting of a research note on the possible exclusion of privacy issues from the February 2017 draft Convention, as well as completing preparatory and drafting work for the WIPO-HCCH Project on developing a resource tool addressing the intersection of private international law and intellectual property law. Furthermore, my internship included preparing presentations on the Judgments Project and the HCCH for international conferences. In addition, I assisted the Permanent Bureau during the February 2017 Special Commission on the Recognition and Enforcement of Foreign Judgments as well as the annual meeting of the Council on General Affairs and Policy of the Conference, organised by the Permanent Bureau. I also assisted the Judgments Team with the preparations of the February 2017 Special Commission and I assisted with minute-taking of an informal meeting during the Special Commission.

During my internship I further developed my research skills and gained valuable knowledge about current private international issues. The experience also inspired the topic of my master’s thesis, especially as I was writing the research note on the possible exclusion of privacy issues from the February 2017 draft Convention on the Recognition and Enforcement of Foreign Judgments. The research note focused both on privacy and data protection matters. It ought to be noted that there is currently no Hague Convention dealing specifically with data protection issues. However, the issue of cross-border data
flown and protection of privacy has been of interest for the HCCH for a long period of time.\textsuperscript{10}

1.2 Objective of the study

Article 3 of the GDPR defines the territorial scope of the GDPR. The provision states the following:\textsuperscript{11}

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.

In this study, Article 3(2) of the GDPR is analysed and examined. Article 3(2) regulates the cross-border situations where the data subject is present in the EU and the controller or the processor is located outside the EU. There are, however, two key criteria that need to be met in order to fall within the scope of the GDPR. As cited above, the processing activities need to be related to the offering of goods or services to data subjects in the EU, or alternatively to the monitoring of the behaviour of those data subjects.


\textsuperscript{11} Emphasis added.
Article 3(2) of the GDPR raises several interesting questions such as:

- Who are the data subjects protected by the GDPR?
- When is the controller or the processor not established in the EU?
- What does “offering goods or services” mean?
- How should “monitoring of their behaviour” be interpreted?

Another challenging fact that arises when analysing data protection issues – in addition to the lack of a binding international instrument regulating the applicable data protection law – is the nature of data protection law. Data protection in cross-border situations does not clearly fall within private or public international law, but instead “straddles the boundaries between public and private law”.12 Whether data protection law should be seen as a part of private or public international law depends on what the particular issue is about, and what kind of activity is in question. Furthermore, the characterisation of data protection issues depends on the parties involved; if all the parties involved are private parties, the data protection issue should be seen as a private law matter.13

Data protection law can therefore be analysed from both a private international and a public international law perspective. This thesis examines the topic from a private international law perspective. Therefore, only the situations where both the data subject and the controller or processor is a private party are of interest for this study. Private international law deals with legal relationships governed by private law, and where the situation in question is connected with more than one country.14

Despite the changes in the GDPR compared to the currently applicable DPD, many principles and characteristics of the DPD are retained in the GDPR.15 Therefore, in order to understand the GDPR, the DPD is of great importance.16 This thesis compares the GDPR with the current legislation in order to evaluate whether the future Regulation is an improvement, when compared with the DPD. Concerning the relation between the

---

12 Bygrave, L, Determining Applicable Law pursuant to European Data Protection Legislation, p 1.
14 Stone, P, EU Private International Law, p 3.
15 De Hert, P, Papakonstantinou, V, Wright, D, Gutwirth, S, The proposed Regulation and the construction of a principles-driven system for individual data protection p 133. See also Chen, J, How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation, p 310.
current and the future legal instrument, recital 171 of the GDPR states that the DPD should be repealed by the GDPR. With regard to processing which is already under way on the date the GDPR becomes applicable, this processing needs to be brought into conformity with the GDPR (recital 171).

This thesis analyses and critically evaluates Article 3(2) of the GDPR, and touches upon the potential consequences of the interpretation and application of the provision. Finally, this study seeks to determine whether the GDPR’s territorial scope has any limits, and if so, how far outside the EU those boundaries can be found.

1.3 Delimitations
The study has its focus on Article 3(2) of the GDPR. Other provisions, such as Article 3(1) of the GDPR will be discussed when necessary in order to determine the territorial scope of the GDPR in cross-border situations. The material scope of the GDPR will not be analysed here. Furthermore, only the private international law aspects of the topic will be discussed in this thesis, and therefore the application of the GDPR in cross-border situations will not be examined from a public international law perspective. Thus, the study will be limited to the question of applicable law. Private international law deals with questions related to applicable law, international jurisdiction and recognition and enforcement of foreign judgments. Since this study is limited to examine when the GDPR is applicable in cross-border situations, the issues of competent courts as well as recognition and enforcement of foreign judgments will not be studied here. Consequently, Article 79(2) of the GDPR dealing with the competent court with regard to proceedings against a controller or a processor will not be discussed here either.

This thesis deals with the private international law aspects of the GDPR, and the focus is therefore on the GDPR and not on private international law instruments. Yet some of the legal instruments in the field of EU private international law will be discussed or touched upon. The concept of ‘directing activities’ appearing both in the Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (‘Rome I Regulation’) and in the Regulation (EU)

---

No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (‘Brussels I bis Regulation’), in the context of consumer law, is of interest for this study. The cases discussed in Chapter 5 regarding the concept of ‘directing activities’ concern the interpretation of Article 15(1)(c) of the Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (‘Brussels I Regulation’), which was later repealed by Brussels I bis Regulation.\(^\text{18}\) Since the wording in Article 17(1)(c) of the Brussels I bis Regulation is the same as in Article 15(1)(c) of the Brussels I Regulation, the case law concerning the Brussels I Regulation is also relevant for the interpretation of the Brussels I bis Regulation.\(^\text{19}\) This thesis will compare the criterion in Article 3(2)(a) of the GDPR with the concept of ‘directing activities’, in order to understand how Article 3(2)(a) is to be interpreted.

Furthermore, the study will touch upon the relationship between the GDPR and the Rome I Regulation in Chapter 5. This is in my view natural since a data subject is sometimes also a consumer in relation to a business. The thesis will, however, not discuss the GDPR in relation to the Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (‘Rome II Regulation’), even though this subject is an interesting and important one. Due to the limited scope of the thesis and the complexity of the relation between the GDPR and the Rome II Regulation, this particular issue will not be dealt with in this study.

On the 27 April 2016 the European Commission published two legal instruments, namely the GDPR and the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.\(^\text{20}\) The Directive 2016/680 is not the subject of this

---

\(^\text{18}\) See Article 80 of the Brussels I bis Regulation.

\(^\text{19}\) See Stone, P, EU Private International Law, p 22-23.

study and will not be touched upon. National data protection laws will not be discussed in this study either.

The territorial scope in Article 3(2) will be analysed in the light of EU case law. I have decided not to discuss the case law of the European Court of Human Rights concerning data protection, even though it is relevant for the interpretation of the GDPR. It is the Court of Justice of the European Union (‘CJEU’) that interprets EU law and therefore the rulings of the CJEU are particularly important and need to be taken into account when interpreting EU law. Due to the limited scope of this study, I have chosen to focus on the cases that are in my view the most relevant ones. The thesis will examine Article 3(2) in the light of the EU cases concerning data protection. Furthermore, EU case law in the field of private international law, consumer law and intellectual property law prove to be of particular relevance.

1.4 Method and sources

The thesis is written from the perspective of EU law and the analysis of Article 3(2) of the GDPR is conducted through the lens of the EU. Thus, the method used in this study is the EU legal method. The topic of the study is Article 3(2) of the GDPR, and the GDPR, which is an EU regulation, is part of EU law. Therefore, it is natural to use the EU legal method when defining the territorial scope of application of the GDPR in cross-border situations.

The EU constitutes a legal order of international law. This was stated by the CJEU in the well-known case Van Gend en Loos (26/62). EU law can be divided in primary law and secondary law. If the hierarchy of EU norms is described as a pyramid, the primary law is at the apex of the pyramid. Primary law consists of the EU Treaties which are the Treaty on EU (‘TEU’) and the Treaty on the Functioning of the EU (‘TFEU’), of the Charter of Fundamental Rights of the EU (‘Charter’) which has the same legal value as the Treaties (Article 6(1) of the TEU), and of the fundamental principles of the EU developed by the

---

22 See section 1.4 below.
The CJEU, including the requirement to protect the fundamental rights recognised in the EU.  

The secondary law includes normative acts adopted by the EU, such as regulations and directives. According to Article 288 of the TFEU, a regulation is binding in its entirety and directly applicable in the EU Member States. A directive is also binding with regard to the result to be achieved, but it leaves to the national authorities the choice of form and methods (Article 288 TFEU). That the DPD will be replaced by a regulation (the GDPR) is a remarkable change regarding the nature of a regulation compared to a directive. The GDPR will be directly applicable in the EU Member States, which is not the case with the DPD.

In order to approach EU law, it is highly important to understand the method that is being used in the analysis. It is difficult to give one single definition to the EU legal method. Thus, the method can be considered as an approach to deal with the legal sources of the EU, listed above. The EU legal method seeks to determine how EU law should be interpreted and applied. Before discussing the interpretation and application of EU law, it is in my view necessary to touch upon the relationship between EU law and the national laws of the EU Member States. According to the principle of primacy, in the case of a conflict, EU law prevails over national law. The primacy of EU law was developed in the Costa v. E.N.E.L. (6/64) case. In addition, EU law has direct effect which means that EU provisions are immediate sources of law for a national court or administrator. For EU law to be applicable within a national legal order there is no need for a further implementing act. The principle of direct effect was established in the Van Gend en Loos case. Interestingly, neither of these two principles, namely the principle of primacy

and the principle of direct effect, appears in the Treaties. Instead, these principles are developed in the case law of the CJEU.\textsuperscript{31}

The CJEU plays an important role in the development of EU law. The CJEU has developed the principles according to which EU law is to be interpreted and applied on a national level.\textsuperscript{32} The fundamental rights codified in the Charter have been developed by the CJEU and mainly in a dialogue with the national courts of the EU Member States.\textsuperscript{33} According to Article 19(1) of the TEU, the Court shall ensure that EU law is observed when interpreting and applying the Treaties. Furthermore, the Court rules on actions brought by a Member State, an institution or a natural or legal person, and gives preliminary rulings which are requested by courts or tribunals of the EU Member States (Article 19(3) of the TEU). The preliminary rulings concern the interpretation of EU law or the validity of acts adopted by EU institutions,\textsuperscript{34} and are binding on the national referring court,\textsuperscript{35} as well as other national courts in the EU.\textsuperscript{36}

In this study, the preliminary rulings of the CJEU on the interpretation of EU law are of great importance and, as already mentioned, Article 3(2) is analysed in the light of relevant EU case law. Since the GDPR will apply from 25 May 2018,\textsuperscript{37} there are currently no preliminary rulings from the CJEU regarding the GDPR. However, the EU case law concerning the current data protection rules of the DPD, as well as other fields of EU law, give valuable guidance to the interpretation of the future legislation.\textsuperscript{38}

The CJEU uses several methods when it interprets EU law, such as the literal interpretation and the teleological interpretation. Thus, it can be noted that especially the teleological method is used by the Court. In the teleological method, provisions are

\textsuperscript{33} Reichel, J, EU-rättslig metod, in: Korling, F, Zamboni, M, Juridisk metodlära, p 117.
\textsuperscript{34} Article 19(3)(b) of the TEU.
\textsuperscript{37} Article 99(2) of the GDPR.
\textsuperscript{38} See Stone, P, Territorial targeting in EU private law, p 14-23.
interpreted in the light of the purpose of the provision. It can be said that the teleological interpretation is based on the doctrine of *effet utile*. According to the doctrine of *effet utile*, the effectiveness of EU law needs to be respected when interpreting and applying EU law. The effectiveness of the GDPR is one of the aspects considered in this study.

The use of the teleological interpretation is apparent in the case law of the CJEU in the field of data protection law. The Court’s interpretation of EU data protection law will be discussed below. Furthermore, the general principles in EU law, such as legal certainty and proportionality, are relevant when discussing and evaluating Article 3(2) of the GDPR.

In order to understand the purpose of a particular provision, the Court uses different tools, including recitals, which are included in the preamble of a legislative act. A preamble consists of everything between the title and the legislative part of an act which is composed of articles. The purpose of the recitals is to provide concise reasons for the provisions. The recitals should, however, not contain normative provisions. Thus, the recitals should be treated with caution, despite the fact that they can be useful in understanding the provisions. The GDPR consists of 173 recitals and 99 articles. As it will be apparent from the analysis in the following Chapters, the recitals clarify the territorial scope of the GDPR and provide detailed explanations.

Surprisingly, the Proposal of the European Commission for the GDPR (Explanatory Memorandum) does not provide any explanations regarding Article 3. Under the

---

41 About the general principles of EU law, see Hofmann, H, General principles of EU law and EU administrative law, in: Barnard, C, Peers, S, European Union Law, p 196-225.
headline “Detailed explanation of the proposal” the European Commission states, concerning Article 3, the following: “Article 3 determines the territorial scope of the Regulation.” It is unfortunate that the European Commission did not provide any detailed explanation for the territorial scope of the GDPR. Thus, the Explanatory Memorandum is not useful in analysing the scope of application of Article 3(2).

Other sources, including academic literature and certain opinions of the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (‘29WP’), are used in the thesis. The academic articles referred to in this study can be found on the internet. The opinions of the 29WP are relevant in order to understand the current data protection rules in the DPD. As noted above, the DPD and the interpretation of its provisions give valuable guidance for the analysis of the GDPR because many of the approaches taken by the GDPR are familiar from the DPD. For example, both the current and the future data protection rules can be described as being principle-driven and human rights- oriented. All in all, the GDPR is in many ways similar to the DPD. Reference is therefore made to the DPD, as well as to the opinions of the 29WP, when it is convenient in order to interpret and to evaluate Article 3(2) of the GDPR.

According to Article 29 of the DPD, the 29WP has an advisory status and it acts independently. The 29WP is composed of representatives of the national supervisory authorities, of a representative of the authorities established for the EU institutions and bodies, and of a representative of the European Commission. The 29WP gives opinions and recommendations on matters relating to the application of the DPD, and contributes to the uniform application of national rules adopted under the DPD. Under the GDPR, the 29WP will be replaced by the European Data Protection Board.

---

49 Chen, J, How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation, p 310; De Hert, P, Papakonstantinou, V, Wright, D, Gutwirth, S, The proposed Regulation and the construction of a principles-driven system for individual data protection, p 133.
50 Article 29(1) and (2) of the DPD.
51 Article 30(1) and (3) of the DPD; Recital 65 of the DPD.
Finally, as noted above, there is currently little literature dealing with the interpretation of Article 3(2) of the GDPR. This is likely due to the fact that the GDPR is not yet applicable, and therefore the CJEU has not interpreted the provision. The novelty and complexity of the subject makes the issue of the territorial scope of application of the GDPR when the controller or the processor is established outside the EU a challenging topic to research. On the other hand, the topic is extremely interesting because the territorial scope of the GDPR in cross-border situations is such a current and important issue.

1.5 Outline

The study begins with an overview of EU data protection law in Chapter 2. The right to data protection is a fundamental right in the EU which will be shortly discussed. The fundamental nature of the right to data protection is relevant in order to understand the GDPR. The developments of EU data protection law since the 1970s until today will be touched upon. As the focus of the thesis is on the territorial scope of the GDPR, it is relevant to discuss the territorial scope of the DPD as well. A short review of the background especially concerning the territorial scope of application is important in order to understand the significance of Article 3(2) GDPR, and why it has been criticised by academics. An introduction to the criteria in Article 3(2) of the GDPR will be discussed after the historic overview.

Chapter 2 is followed by two chapters, namely Chapters 3 and 4, concerning the persons covered by Article 3(2) of the GDPR. This is relevant in order to analyse the territorial scope of application of the GDPR and the questions it gives rise to. In addition, to know who is covered by Article 3(2) is relevant in order to understand what potential disputes may arise, and between which parties, when applying Article 3(2) GDPR. In Chapter 3, the question of who the data subjects protected by the GDPR are, will be discussed. Chapter 4 seeks to determine when a controller or a processor is not established in the EU.

After Chapters 3 and 4, the focus of the thesis will shift to the two main criteria in Article 3(2) of the GDPR. According to Article 3(2)(a), the GDPR is applicable when the controller or the processor is offering goods or services to data subjects in the Union,
which is the subject of Chapter 5. This criterion will be analysed in the light of CJEU case law. In Chapter 6, Article 3(2)(b) and its criterion, the monitoring of the behaviour of data subjects in the EU, will be analysed. The conclusions of the study will be presented in Chapter 7.
2 EU data protection law

2.1 The fundamental right to data protection and its legal basis

2.1.1 Article 16 of the TFEU and Article 8 of the Charter

The GDPR has its legal basis in Article 16 of the TFEU, according to which everyone has the right to the protection of personal data concerning them (Article 16(1) TFEU). Article 16 gives the EU a mandate to legislate in order to guarantee the right to data protection.\(^{53}\)

The right to data protection is a fundamental right in the EU and it is included in the Charter. According to Article 8(1) of the Charter, everyone has the right to the protection of personal data concerning him or her.

The GDPR highlights the fact that the right to data protection is a fundamental right within the EU. The Regulation starts by stating, in recital 1, that the protection of natural persons in relation to the processing of personal data is a fundamental right, and refers to Article 16 of the TFEU as well as to Article 8 of the Charter. Furthermore, the objective of the GDPR is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data (Article 1(2) GDPR).

The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community made the Charter a legally binding instrument and the Charter was incorporated into EU law, as part of the Treaty.\(^{54}\) Before the Charter became legally binding in 2009,\(^{55}\) the CJEU referred in its case law to the fundamental rights recognised in the European Convention on Human Rights (‘ECHR’). Despite the fact that there is no reference to the ECHR in the preamble of the GDPR, the ECHR is relevant when interpreting the GDPR. The Convention rights and the fundamental concepts of EU law are important in the interpretation of the GDPR. Concepts such as equality, legal certainty, fundamental rights and proportionality need to be taken into account. The rights

---


\(^{55}\) Article 6 of the Treaty of Lisbon.
covered by the ECHR are recognised in Article 6 of the Treaty of Lisbon and they are considered as general principles in EU law.\textsuperscript{56}

\textbf{2.1.2 Data protection and privacy – two separate rights}

While the right to data protection is protected under Article 8 of the Charter, the right to respect for private and family life is protected under Article 7 of the Charter. The right to respect for private and family life is also recognised in Article 8 of the ECHR. Thus, the right to data protection on the one hand and the right to privacy on the other are two distinguished rights. These two rights are therefore not identical but are similar to each other.\textsuperscript{57}

Likewise, the GDPR expressly makes the distinction between these two rights in recital 4 where it is stated that the GDPR “respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, (…)”

The right to privacy can be considered a broader concept than the right to data protection because it covers all matters related to one’s private life. This also includes the protection of the personal data of an individual as long as this data falls within the sphere of one’s private life.\textsuperscript{58} It can be said that data protection is “one of the aspects of the right to respect for private life”.\textsuperscript{59}

Hence, the concept of privacy does not cover all information on identified or identifiable persons. In other words, all the personal data that falls within the scope of data protection


\textsuperscript{57} Kokott, J, Sobotta, C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR, p 223; Leenes, R, Van Brakel, R, Gutwirth, S, De Hert, P, Data Protection and Privacy: (In)visibilities and Infrastructures, p 3-4.


\textsuperscript{59} Case T-194/04, Bavarian Lager v. Commission, para 118.
is not necessarily considered as part of one’s private life. Therefore, it can also be argued that the scope of the right to data protection is broader than the right to privacy since it covers all personal data of a natural person, including the information that is not included in one’s private life.

2.1.3 A fundamental right – but not an absolute right
That both the right to data protection and the right to privacy are fundamental rights under EU law does not mean that these rights are absolute. Recital 4 of the GDPR states that the right to data protection needs to be considered in relation to its function in society and needs to be balanced against other fundamental rights, according to the principle of proportionality. Furthermore, the Charter concedes that the right to data protection can be limited under certain conditions. Article 52(1) of the Charter states that any limitations on the exercise of the fundamental rights recognised in the Charter must be provided by law, and are permissible only if they are necessary and genuinely meet objectives of general interests recognised by the EU or, alternatively, the need to protect the rights and freedoms of others.

2.1.4 Is there a fundamental right to data protection in horizontal situations?
An interesting question is whether the fundamental right to data protection also applies when both parties are private persons. The controller or the processor who is processing the personal data of data subjects in the EU are often large private companies established in third states, with a strong market position. Thus both parties, a data subject on the one hand and a controller on the other, are private parties. This study has its focus on these kinds of scenarios, since the analysis is limited to the private international law aspects of Article 3(2) of the GDPR. Cases where both parties are private parties fall under private law and are considered as horizontal situations. It is, however, unclear whether the Charter applies to purely horizontal situations. The question is whether the Charter is

60 Kokott, J, Sobotta, C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, p 225.
directly binding on private parties. Due to the complexity of this issue and the fact that it is not the topic of this study, it will only be commented upon here shortly.

There are several arguments that support the horizontal effect of the Charter, one of them being that the possible misuse of personal data by the private sector was one of the reasons behind the development of special EU data protection rules in the 1970s. However, even if the Charter would not have direct effect in situations involving private parties, the Charter may be indirectly applicable. This is because EU law is interpreted in the light of the Charter. It can also be argued that governments have a positive duty to protect the fundamental rights of individuals, and to ensure that these rights are effectively protected also in horizontal situations. In the context of the internet, the controllers and the processors are often private companies that are dominant economic players. The fundamental right to data protection would be ineffective if data subjects were only protected against governments and state actors, and not against these private companies. It would, in my view, not be justified if the legislation provided a different degree of protection depending on whether the controller was a state actor or a private company.

Regardless of whether the Charter is applicable in horizontal situations, the GDPR applies in public sector as well as in private sector. This is apparent from the general provisions in the GDPR which do not distinguish between public and private sector. Consequently, the GDPR protects the fundamental right to the protection of personal data of data subjects in the EU, regardless of whether the controller or the processor is a state actor or a private company.

---

64 Hijmans, H, The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU, p 37; Explanatory Report for the Protection of Individuals with regard to Automatic Processing of Personal Data, para 4.
2.2 An historic overview of the data protection legislation in Europe

2.2.1 Developments since the 1970s

Technology has been challenging law-making for the past forty years. In Europe, the first legislation in the field of data protection was introduced in Germany, in the state of Hesse, in 1970. Furthermore, the first nationwide data protection legislation was introduced in Sweden in 1973, followed by Germany and France some years later.

On a European level, the Council of Europe has had an active role in the development of data protection law. The data protection law developed first in the context of Council of Europe and later in the context of the EU. In the early 1970s, the Council of Europe found that the national legislations did not provide a sufficient protection to individual privacy and other rights regarding the automated data banks. As a result, the Committee of Ministers to the Member States adopted two recommendations, namely the Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector in 1973, and Resolution (79) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector in 1974. The Council of Europe continued working on this field of law and adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention 108’) in 1981. The purpose of the Convention 108 is according to its Article 1 to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (‘data protection’). The Convention 108 is currently ratified by all EU Member States.

---

The European Commission considered the Convention 108 as an opportunity to set up common ground rules in the EU. Thus, the European Commission issued a recommendation, namely the 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, encouraging the Member States to ratify the Convention 108 before the end of 1982. However, the Convention 108 did not succeed in ensuring sufficient consistency within the EU. While some Member States were late in implementing the Convention 108, other Member States that had implemented the Convention 108 had arrived at different outcomes. Due to this lack of consistency, the European Commission was concerned about the development of internal market in several areas where the processing of data had a significant role. Consequently, the European Commission adopted the current Data Protection Directive in 1995 in order to harmonise the national laws within the EU.

2.2.2 The Data Protection Directive (DPD)

The DPD has two main goals. Firstly, its objective is to achieve a minimum level of data protection within the EU. Secondly, by allowing the free data flows within the EU, it seeks to prevent the Member States from blocking inter-EU data flows on data protection grounds. Thus, one of the aims of the DPD is to protect individuals’ right to data protection. This objective is a result of an increased concern for the protection of the fundamental right to data protection.

Furthermore, there was a need for a direct action from the European Commission due to the existing divergences between different national data protection legislations. In some Member States there was no legislation at all on this area of law. These differences on the national level were an obstacle for cross-border flow of data and the DPD was a tool to

---

eliminate these obstacles. Therefore it can be said that the DPD aimed at improving the functioning of the internal market.\footnote{Lynskey, O, Foundations of EU Data Protection Law, p 49-50.}

In addition to its contribution to the functioning of the internal market of the EU, the application of the DPD may have third country implications. The DPD regulates the transfer of personal data, not only from one Member State to another, but also from EU Member States to third countries. Data transfers from an EU Member State to a third country are allowed only if the third country in question has an adequate level of data protection,\footnote{Article 25(1) of the DPD.} or if the data processing is expressly exempted from the scope of the Directive.\footnote{Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 21.} Articles 25 and 26 of the DPD regulate the transfers of personal data to third countries. Corresponding provisions can be found in Articles 44 to 50 of the GDPR, which deal with transfers of personal data to third countries or international organisations. It is worth noting here that the GDPR recognizes the importance of cross-border data flows. The GDPR states in recital 101 that flows of personal data between the EU and third countries are necessary for the expansion of international trade and international cooperation.

When the rules on jurisdiction and conflict of laws in Article 4 (cited below) of the DPD were drafted, the primary goal was to ensure free information flows within the European common market, but not outside those borders.\footnote{Kuner, C, Transborder Data Flows and Data Privacy Law, p 110-111.} During the drafting process, processing of personal data outside the EU was not sufficiently taken into consideration which resulted in more or less unclear rules on applicable law and jurisdiction. In addition, as Kuner notes, “most of the controversies surrounding European data protection law have been caused by the fact that legal instruments designed mainly for intra-EU use have been forced by the expanding information economy to be applied to global problems on a scale for which they were not intended”.\footnote{Kuner, C, Transborder Data Flows and Data Privacy Law, p 111.}

More or less every data transfer is in today’s world international, and global aspects of data protection have received more attention than before.\footnote{Kuner, C, Transborder Data Flows and Data Privacy Law, p 111.} The technology has led to an
increased processing of individuals’ personal data outside the EU.\textsuperscript{85} There are therefore good reasons for applying the data protection law also to the processing of data by a controller outside the EU. A relevant question is, however, \textit{when} the EU data protection legislation applies to the processing of personal data, when the controller is established outside the EU. Article 4 of the DPD provides the territorial scope of the DPD and defines when the DPD applies to the processing of personal data.

According to Article 4(1) of the DPD,\textsuperscript{86}

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   a) the processing is carried out \textbf{in the context of the activities of an establishment} of the controller \textbf{on the territory of the Member State}; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   b) the controller is \textbf{not established} on the Member State’s territory, but in a place where its national law applies by virtue of international law;
   c) the controller is \textbf{not established} on Community territory and, for purposes of processing personal data \textbf{makes use of equipment}, automated or otherwise, \textbf{situated on the territory of the said Member State}, unless such equipment is used only for purposes of transit through the territory of the Community.

It has been noted that Article 4 of the DPD has a double function since it not only determines which Member State’s law is the applicable law, but also \textit{when} one Member State’s law is applicable “as opposed to the law of a third country”.\textsuperscript{87} Article 4(1)(a) is applicable when the controller has an establishment in the EU, whereas Article 4(1)(b) and (c) apply when the controller is not established in the EU. Article 4(1)(a) and (c) of the DPD are based on the territoriality principle since the connecting factor activating the application of the DPD is the location of either the establishment of the controller (a) or


\textsuperscript{86} Emphasis added.

\textsuperscript{87} Brkan, M, Data Protection and European Private International Law, p 32.
the equipment used in the processing of personal data (c); the establishment or the equipment needs to be located within the EU.\textsuperscript{88}

2.3 The GDPR and its new criteria

2.3.1 The GDPR provides new aspects to EU data protection law

The GDPR introduces new factors that connect a cross-border situation with the EU territory (‘connecting factors’). A connection with the EU is necessary for the GDPR to be applied when a third country is involved. A significant change is made when comparing the determination of the territorial scope of the GDPR in Article 3(2) to the territorial scope of the DPD in Article 4(1)(c). Instead of referring to the use of equipment situated on EU territory, as in Article 4(1)(c), the GDPR introduces new connecting factors\textsuperscript{89} such as the offering goods or services \textit{to data subjects in the Union} and the monitoring of their behaviour as far as \textit{their behaviour takes place within the Union}.

Interestingly, the GDPR adds a destination approach to the territoriality approach. The territoriality principle can still be found in the GDPR but it is not as explicit as in the DPD.\textsuperscript{90} Also, it can be noted that the GDPR does not refer to the territory of the EU, but instead uses the expression “in the Union”. In my view, “in the Union” has the same meaning as ‘on the territory of the EU’. The territorial scope of the GDPR would therefore be the same even if the GDPR would require that the data subject is within the territory of the EU. However, the EU legislator seems to avoid using the term ‘territory’. GDPR’s territorial scope will be discussed in detail in the following Chapters.

Due to the increased cross-border data flows, the principle of territoriality is losing its importance in private international law. A strict application of the territoriality principle does not work in the internet context.\textsuperscript{91} While the localisation of activities in the physical world is comparatively easy to carry out, it can be impossible to localise activities taking

\textsuperscript{88} Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, p 29.
\textsuperscript{89} De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 236.
\textsuperscript{90} De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 231 and 236.
\textsuperscript{91} Svantesson, D, Private International Law and the Internet, p 8-9.
place on the internet. This is because the internet has no territorial boundaries, and its geography is virtual. In order to determine which court has jurisdiction and which law is applicable, private international law provides connecting factors. The rules on applicable law and jurisdiction in private international law depend on the localisation of activities and persons. As a result, the connecting factors generally used in private international law to determine the applicable law and jurisdiction are not always suitable in an online context.\(^{92}\)

A noted in Chapter 1, the new approach to the territorial scope in the GDPR is an important change in the GDPR, compared to the DPD. Article 4 of the DPD does not give sufficient protection to the data subjects in the EU, when the controller or the processor is established outside the EU. Due to rapid technological development, personal data is constantly processed by controllers in third countries. The new techniques to target and track data subjects online has raised concerns as to how to protect these individuals from the processing of their data by controllers outside the EU.\(^{93}\) These concerns led to a broader territorial scope in Article 3(2) of the GDPR, compared to the DPD.\(^{94}\) The controller or the processor cannot escape the rules of GDPR by moving its establishment to a third country or by not using any equipment in EU territory. Instead, what is relevant is whether the business is offering goods or services to data subjects in the EU, or monitoring their behaviour.

2.3.2 Who is covered by the GDPR?
Before analysing the two conditions in Article 3(2) of the GDPR, it is highly relevant to discuss which persons are covered by the GDPR. This is necessary in order to determine who the potential claimants and defendants in a data protection dispute may be.\(^{95}\) As the thesis takes into consideration solely the private international law aspects of the topic, only situations where private parties are involved are of interest here.

\(^{92}\) Reed, C, Internet Law, p 217-219.
\(^{93}\) See Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, p 28 and 43-44.
\(^{94}\) See De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 231.
\(^{95}\) Brkan, M, Data Protection and European Private International Law, p 259.
In cross-border data flows from the EU to third countries it is evident that one of the parties needs to be located in the EU and the other outside the EU. In the case of the GDPR, the territorial application of the Regulation outside the EU requires that the data subject is in the Union. The data controller or processor is, on the other hand, not located in the EU. In other words, Article 3(2) applies when the controller or the processor is not established in the EU.

As the title of the GDPR implies, the GDPR regulates the protection of natural persons with regard to the processing of personal data. According to Article 4(1) of the GDPR, a ‘data subject’ is an identified or identifiable natural person. The parties involved are therefore a natural person being the data subject on the one hand, and the controller or processor on the other. The parties will be further defined in the following Chapters.

The GDPR is applicable when a controller or a processor has an establishment in the EU, and also – under certain conditions – when the controller or processor has no establishment in the EU. Article 3 of the GDPR defines the territorial scope of the GDPR and distinguishes, as does the DPD, between these two types of situations, Article 3(1) being applicable when the controller or the processor is established in the EU, and Article 3(2) when the controller or the processor is not established within the EU.\footnote{See Brkan, M, Data Protection and Conflict-of-laws: A Challenging Relationship, p 336.} Chapter 3 deals with data subjects in the EU, and Chapter 4 focuses on determining when a controller or a processor is not established in the EU.
3 Data subjects in the EU

3.1 Natural persons enjoying the protection of the GDPR

Personal data of *natural persons* is protected by the GDPR which is clearly stated in the title of the GDPR, as well as in the articles and recitals.\(^{97}\) Interestingly, the notion of a ‘natural person’ is not defined in Article 4 (‘Definitions’) or anywhere else in the GDPR. In order to determine whether a person falls within the scope of the Regulation, it is important to know whether the person is considered a ‘data subject’ or not. Is it necessary that the data subject is an EU citizen, or that this person has his or her residence in the EU? What is a sufficient connection with the EU, for the Regulation to be applicable? These and other questions will be discussed in this Chapter.

3.1.1 Who is a data subject according to the GDPR?

The definition of personal data in Article 4 of the GDPR provides some kind of a definition to the notion of ‘data subject’. Article 4(1) states that “any information relating to an identified or identifiable natural person (‘data subject’)” is considered as personal data. This definition appears to be directly taken from Article 2(a) of the DPD. Furthermore, Article 4(1) of the GDPR clarifies that “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. This list appears to be a non-exhaustive list, which however includes a variety of different identifiers. In my view, this definition gives a clear picture of what kind of factors are to be considered as identifiers within the meaning of the GDPR.

Concerning the DPD, the 29WP argues in one of its opinions that ‘natural persons’ means human beings.\(^{98}\) Furthermore, the 29WP refers to Article 6 of the Universal Declaration of Human Rights which states that “everyone has a right to recognition everywhere as a

\(^{97}\) See for example recitals 1 and 2, and Article 1 of the GDPR.

person before the law”.\textsuperscript{99} Hence, the 29WP notes that the DPD is, in principle, applicable to living individuals only.\textsuperscript{100}

A difference between the GDPR and the DPD is that the DPD does not explicitly mention deceased persons. Since dead individuals are not natural persons in civil law, the same applies in principle in data protection law. Nevertheless, the 29WP notes that deceased persons can indirectly be protected by the DPD, for example when the information about the deceased person refers to a living individual. In addition, Member States may extend the scope of their national data protection law (when implementing the DPD) so that it also includes the processing of data on deceased persons.\textsuperscript{101}

Unlike the DPD, the GDPR expressly states in recital 27 that personal data of deceased persons is excluded from its scope. Therefore, deceased persons are also excluded from the definition of natural persons. However, Member States are allowed to provide national rules regarding the protection of deceased persons and their data (recital 27 of the GDPR).

When it comes to unborn persons, the GDPR as well as the DPD, is silent. The 29WP comments this issue by stating that whether unborn children are protected by data protection law depends on the general position taken in the Member States concerning the protection of unborn children. Whether information on unborn children is protected by the national legislations, both that general position and the purpose of data protection rules to protect the individual should be taken into consideration.\textsuperscript{102} It can be argued that since the GDPR expressly mentions that the Member States can legislate on the protection of deceased persons, the same should reasonably apply to the issue of unborn children and the protection of information related to them.

Furthermore, Kuner points out that it is not apparent from the DPD whether it excludes the processing of data of legal persons.\textsuperscript{103} Recital 24 of the DPD states that the DPD does not affect the legislation concerning protection of legal persons and processing of data

\begin{itemize}
\item \textsuperscript{99} United Nations, Universal Declaration of Human Rights, 1948.
\item \textsuperscript{100} Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p 21-22.
\item \textsuperscript{101} Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p 22.
\item \textsuperscript{102} Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p 23.
\item \textsuperscript{103} Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 77.
\end{itemize}
related to them. Kuner argues that the DPD allows the Member States to extend the protection of their national legislation also to legal persons.\textsuperscript{104}

The GDPR is, however, very clear in its recital 14 that the GDPR does not cover the processing of personal data which concerns legal persons. Recital 14 states that the Regulation does not cover the processing of personal data concerning legal persons, in particular “undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.” Despite this, it can be difficult to determine whether information is related to an individual being a natural person in the meaning of the GDPR, or to the individual as a legal person. This can be particularly difficult with a person who is alone the proprietor of a small business.\textsuperscript{105}

Drawing the line between information related to the personal life of an individual on the one hand and information related to the work of the individual on the other can be challenging, for example when the same e-mail address or social media account is used for both private and professional purposes. Thus, it can be difficult to determine whether information in an e-mail should be considered as part of one’s private life or as part of one’s professional life.\textsuperscript{106} Whether the data is ‘personal data’ depends on this qualification of the information in question.

Additionally, the data controller might process and collect data on natural and legal persons including them in the same sets of data. These situations will probably result in applying the data protection rules to all data instead of trying to separate the information that refers to a natural person on the one hand and to a legal person on the other.\textsuperscript{107}

With the DPD, this differentiation between natural and legal persons is left to national courts.\textsuperscript{108} With the GDPR, it is to the CJEU to decide where the borderline goes, since the GDPR should be interpreted uniformly in the EU and the CJEU has, as noted above, a decisive role in determining how EU law is to be interpreted.

\textsuperscript{104} Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 77.
\textsuperscript{105} Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 77.
\textsuperscript{106} See Brkan’s reasoning in the context of consumer law in: Brkan, M, Data Protection and European Private International Law, p 13-14.
\textsuperscript{108} See Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 77-78.
3.1.2 The significance of nationality and residence

According to recital 2, the GDPR applies to the processing of personal data of natural persons regardless of their nationality or residence. A corresponding sentence can also be found in the DPD.\(^{109}\) The 29WP states in one of its opinions that everyone has a right to data protection under EU law.\(^{110}\) In another opinion 29WP notes that it would not be acceptable “to reduce the scope of protection to persons residing in the EU, since the fundamental right to protection of personal data is enjoyed regardless of nationality or residence”.\(^{111}\)

As stated in the Draft Charter of Fundamental Rights of the European Union, text of the explanations relating to the complete text of the Charter, the dignity of the human person constitutes the real basis of fundamental rights.\(^{112}\) The text of explanations refers to the 1948 Universal Declaration of Human Rights which states in its preamble that: “Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world”.\(^{113}\)

Similarly, the GDPR seems to cover all human beings present in the EU.

Consequently, an individual who has his or her residence outside the EU and who is visiting the EU is considered a ‘data subject’ in the meaning of the GDPR, under the condition that his or her personal data is being processed during that visit in the EU. For example, the GDPR would protect the personal data of a person, who has his or her residence in the US, when on holidays in Paris. This US resident buys clothes online from a hotel room and meanwhile her or his personal data is being processed by the website in question. The controller, established in the US, would need to comply with the rules of the GDPR.\(^{114}\) In my view, this particular situation has a stronger connection with the US

\(^{109}\) According to recital 2 of the Directive “data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals”.

\(^{110}\) Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and Inc v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González” C-131/12, p 3.


\(^{112}\) Draft Charter of Fundamental Rights of the European Union - Text of explanations relating to the Charter, explanation on Article 1.

\(^{113}\) United Nations, Universal Declaration of Human Rights, preamble (emphasis added).

than with the EU. This is because the natural person lives in the US and the controller is established in the US. The only connection with the EU is that the personal data is being processed while the natural person is present in the EU.

However, the GDPR is very clear that the nationality or the residence of a data subject is irrelevant in order to determine whether the GDPR is applicable. It seems that the mere fact that the person is physically present in the EU when the processing takes place is the determining factor.\textsuperscript{115}

3.1.3 Data subjects physically present in the EU

Article 3(2) of the GDPR requires that the data subject is in the Union. There is no such requirement in Article 4 of the DPD. The DPD applies regardless of the physical presence of the data subject. Instead, the decisive factor in the DPD, when the controller is not established in the EU, is the location of the equipment used by the controller.\textsuperscript{116} Thus, regarding cross-border situations, the legislator has shifted the focus from the location of the controller and its equipment to the physical presence of the data subject. Interestingly, the approach taken in the DPD is retained in Article 3(1) of the GDPR which regulates situations involving a controller or processor established in the EU.

Article 3(1) states that the GDPR is applicable to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. This provision does not require that the natural person, whose personal data is being processed, is physically present in the EU. What is required is that the controller or the processor is in the EU. Article 3(2), in turn, rules that the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or a processor not established in the EU. This provision expressly requires that, when the controller or the processor is not established in the EU, the data subject needs to be in the EU. It can be noted that the connecting factors are different in Article 3(1) and Article 3(2); the former having the

\textsuperscript{116} See Article 29 Data Protection 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 websites, p 7.
establishment located in the EU as a connecting factor, while the latter uses the presence of the data subject within the EU territory as a required connection with the EU.

It seems that when the controller or the processor is established in the EU, this is a sufficient connection with the EU. When the controller or the processor is instead not established in the EU, the data subject needs to have a connection with the EU territory, and according to Article 3(2) this connection exists when the data subject is in the Union. Article 3(2) is well in line with recital 2 stating that the GDPR applies regardless of the nationality or residence of the data subject. Hence, it is unclear what is actually required, how strong of a connection with the EU is sufficient, in order to fall within the scope of the GDPR. Is it enough to be only temporarily present in EU, in order to be considered a data subject? Or are there further requirements? In my view, the wording of the GDPR indicates that the mere presence on the EU territory is sufficient. This can, in my opinion, be criticised since the situations where the data subject is only temporarily visiting the EU may have a stronger connection with a third country, for example with the state where the controller is established. Such a stronger connection exists in my view in the example mentioned above, where a US resident buys goods online, from a US company, while being physically present in Paris. On the other hand, that the GDPR covers not only the EU citizens and residents but also persons temporarily present in the EU is understandable taken into account the fact that the right to the protection of personal data is a fundamental right, as discussed above.

Finally, it can be argued that according to a very extensive interpretation of Article 3(2), the Regulation could apply when an EU resident buys goods or uses services while being physically present within a third state territory. I agree with Brkan that such an extensive interpretation would, however, be against the wording in Article 3(2) of the GDPR. As underlined above, the GDPR expresses clearly that it is the physical presence of the data subject within the territory of the EU that is the determining factor for the applicability of the GDPR, and not the nationality or residence of the data subject.

---

4 Establishment and its implications

The location of the establishment of a controller or a processor is a determining factor for the applicability of Article 3(1) and Article 3(2) of the GDPR. Since the topic of the study is the territorial scope of the GDPR when the controller or the processor is not established in the EU, the focus in this section is on the concept of ‘establishment’. Article 3 of the GDPR distinguishes between the two different types of situations depending on the location of the establishment and determines whether Article 3(1) or Article 3(2) is to be applied. However, before analysing the notion of ‘establishment’, the terms ‘controller’ and ‘processor’ will be briefly discussed.

4.1 Controllers and processors

The GDPR as well as the DPD divides the actors, who are processing data, to data controllers and data processors. According to Article 4(7) of the GDPR, a controller is “the 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”. Furthermore, Article 4(8) of the GDPR states that ‘processor’ is defined as “a natural person or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. In the private sector, the controller or the processor is generally either a natural or a legal person. Article 2(2)(c) excludes from the scope of the GDPR the processing of personal data by a natural person in the course of a purely personal or household activity. Recital 18 further clarifies that in these situations there is no connection to a professional or commercial activity.

Surprisingly, the CJEU found in the Bodil Lindqvist (C-101/01) case that a situation where a private person publishes information about other persons on the internet falls within the scope of the DPD. In this case, an individual named Bodil Lindqvist had published information about herself and her 18 colleagues in the parish where she was working. The information was published on internet pages that she had set up herself, and

---

118 See Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 69.
120 Case C-101/01 para 48. See also Council of Europe, European Union Agency for Fundamental Rights, Handbook on European data protection law, p 49.
had requested to have a link between those pages and the Swedish Church’s website. She had set up the internet pages in order to provide parishioners, preparing for their confirmation, with information they may need. On these pages, she referred to her colleagues by including either their full names or only first names. She described their jobs and hobbies in a rather humorous manner. In many of the cases she even mentioned family circumstances and telephone numbers. Concerning one of the colleagues she informed that this colleague was working half-time on medical grounds because she had injured her foot.\textsuperscript{121}

The Court ruled in this case that the processing of personal data was not excluded from the scope of the DPD since the provision in question (Article 3(2) of the DPD) must be interpreted “as relating only to activities which are carried out in the course of private life or family life of individuals, which is clearly not the case with processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.”\textsuperscript{122} The Court’s ruling in the \textit{Bodil Lindqvist} case should, in my view, be relevant even when interpreting the GDPR since the exclusion in Article 3(2) of the DPD is also present in Article 2(2)(c) of the GDPR. It can be noted that the wording concerning this particular exception is in general the same in the DPD and in the GDPR, except that the latter has added in recital 18 that the GDPR does apply to controllers or processors which provide the means for processing of personal data for such personal or household activities.

\section*{4.2 Establishment as a key concept}

As mentioned above, Article 3 of the GDPR distinguishes between situations where the controller or the processor is established in the EU on the one hand and situations where these actors are not established in the EU on the other.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{121} Case C 101/01 para 12 and 13.
\item \textsuperscript{122} Case C 101/01 para 47.
\end{itemize}
\end{footnotesize}
Article 3(1) states that:’’ 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.”

According to Article 3(2), the 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 (…)” Furthermore, Article 3(2) sets further requirements in Article 3(2)(a) and (b).

It is worth noting that in the online context it might be difficult to determine where a controller or a processor is established. It can also be questioned whether a website can be considered as an establishment. These issues will not be analysed here but it can, however, be noted that Article 3(2) does not require that the controller or the processor has an establishment in a third country. Instead, Article 3(2) is applicable when the controller or the processor is not established in the EU. Whether a controller is established in the EU, on the other hand, has been dealt with in EU case law. Therefore, the question whether an establishment exists in a third country should not be problematic here.

To determine when a controller or a processor does not have an establishment in the EU, it is necessary to discuss what is required in order to have an establishment in the EU. In other words, this section seeks to determine what an ‘establishment’ means in order to understand which situations fall within Article 3(1) on the one hand, and Article 3(2) on the other.

According to recital 22 of the GDPR, an establishment refers to “the effective and real exercise of activity through stable arrangements”. Furthermore, recital 22 states that “the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect”. A corresponding definition can be found in recital 19 of the DPD. As noted by Kuner, the definition of an establishment is rather broad. It does not only include permanent establishments such as corporate entities, but also other types of business activities indicating a durable connection with a forum. However, there are also many activities relevant to e-commerce that are not

---

123 Emphasis added.
124 Emphasis added.
125 Bygrave, L, Determining Applicable Law pursuant to European Data Protection Legislation, p 9.
considered as EU-based establishments, for example maintaining a website that is located outside the EU but accessible to users in the EU. Then there are some grey areas too. As falling within the grey area, Kuner includes online advertising directed to Europeans that does not necessarily fulfil the requirement of stable presence of the actor in the EU, but which might nevertheless be economically significant.\footnote{Kuner, C, European Data Protection Law: Corporate Compliance and Regulation, p 83.} These kinds of situations will, in my opinion, no longer be problematic with the GDPR due to its Article 3(2), since the online advertising would be considered as offering goods or services to data subjects in the EU or as a result of the monitoring of the behaviour of those data subjects. Due to Article 3(2) of the GDPR the situations lacking stable presence in the EU - and described as grey areas by Kuner - vanishes, at least when it comes to online advertising and similar activities.

A flexible definition to an ‘establishment’ was given by the CJEU in the case of Google Spain and Google (C-131/12), followed by the Weltimmo (C-230/14) case. In these two cases, the Court took a broad approach on territoriality. As a result, a certain level of physical presence of a third state company on the territory of the EU can force the company to comply with the EU data protection rules.\footnote{De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 233.} The following sections 4.2.1 and 4.2.2 focus on the definition of an ‘establishment’ given by the CJEU.

4.2.1 Google Spain and Google

In the Google Spain and Google case, the dispute in the main proceedings concerned personal data of a Spanish national resident, Mr Costeja González, appearing in links to the daily newspaper La Vanguardia. When Mr González’s name was entered by an internet user on Google’s search engine, links to two pages of La Vanguardia’s newspaper would appear, these pages mentioning Mr González by name. He was mentioned in relation to a real-estate auction which had a connection with attachment proceedings concerning the recovery of social security debts.\footnote{Case C-131/12 para 14.} In his complaint Mr González requested that his personal data would be removed or that this personal data would no longer appear in the links to La Vanguardia. The national court of Spain, where the
proceedings had been initiated, requested a preliminary ruling and referred three questions to the CJEU. The first of them regarding the territorial scope of the DPD, and more precisely the interpretation of Article 4(1)(a) DPD, is of interest here. The other questions will not be discussed since they fall beyond the scope of this study.

The first question centered around the interpretation of an ‘establishment’. Three possible scenarios were given by the national court in order to concretise the question. The national court started with asking whether it is to be considered as an ‘establishment’ when “the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State”. The Court noted that Article 4(1)(a) should not be interpreted restrictively and that the provision prescribes a particularly broad territorial scope. The Court’s reasoning was mainly focused on determining the meaning of “in the context of the activities” of an establishment, instead of the notion of ‘establishment’.

The Court stated that ‘carried out in the context of the activities’ in Article 4(a) of the Directive cannot be given a restrictive interpretation, since the provision needs to be read in the light of the objective of the DPD. Furthermore, the Court noted that the objective of the DPD is to ensure the effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.

When it comes to the notion of ‘establishment’, the Court stated the following: “It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an ‘establishment’ within the meaning of Article 4(1)(a) of the Directive 95/46.” Furthermore, the Court concluded that there is an establishment when the operator of a search engine sets up a branch or a subsidiary in a Member State. Recital 19 of the DPD (recital 22 of the

---

129 Case C-131/12 para 20.
130 Case C-131/12 para 54.
131 Case C-131/12 para 53.
132 Case C-131/12 para 49.
133 Case C-131/12 para 60.
GDPR) states, however, that the legal form of the establishment, being a branch or a subsidiary, is not a determining factor. The Court’s short reasoning in this regard does not further clarify what is required in order to be considered an establishment. The Court seems to give a flexible definition to the provision but it does not specify what the flexible definition means for the notion of ‘establishment’.

4.2.2 Weltimmo
The CJEU brought further clarity to the definition of an establishment in its judgment in the case of Weltimmo. The dispute in main proceedings was between Weltimmo s.r.o. (‘Weltimmo’), a company registered in Slovakia, and the Hungarian data protection authority. The dispute concerned a fine imposed by the Hungarian data protection authority for infringement of the Hungarian law on the right to self-determination as regards information and freedom of information which transposed the Directive 95/46 into Hungarian law. Weltimmo ran a property dealing website concerning Hungarian properties, and therefore processed the personal data of the advertisers. Several advertisers had requested the deletion of their advertisements as well as their personal data from the period the advertisements became payable. The advertisements were namely free of charge for one month and thereafter payable.

Hence, Weltimmo did not delete the personal data that was requested to be deleted and, since the advertisers did not pay the price for the services, forwarded their personal data to debt collection agencies. The advertisers complained about Weltimmo to the Hungarian data protection authority which then imposed a fine on that company. Consequently, Weltimmo brought an action before the Budapest administrative and labour court which ruled in favour of the Hungarian data protection authority and stated that since the processing of data and the supply of data services related to the Hungarian property had taken place in Hungary, the fact that Weltimmo was not registered in Hungary was not a valid argument in defence. Weltimmo appealed to the Supreme Court of Hungary which referred questions to the CJEU for a preliminary ruling.

---

134 Case C-230/14 para 2.
135 Case C-230/14 para 9.
136 Case C-230/14 para 9-14.
The relevant question for this study concerned the interpretation the notion of ‘establishment’ in Article 4(1)(a) of the DPD. The Court found that Article 4(1)(a) permits the application of the law on the protection of personal data of a Member State other than the Member State in which the controller is registered considering that the controller exercises, through stable arrangements within the territory of that Member State, a real and effective activity in the context of which the processing of the personal data is carried out. The Court referred to the opinion of Advocate General Cruz Villalón who had noted that the notion of ‘establishment’ was given a flexible definition in recital 19 of the DPD (recital 22 of the GDPR). Furthermore, he had stated that this definition departs from a formalistic approach, whereby undertakings are established solely in the place where they are registered. He had noted that the criterion of effectiveness and permanence are present in the definition, by requiring “the effective and real exercise of activity through stable arrangements”. Furthermore, by adding in the recital that the legal form of an establishment is not a determining factor, the legislator expressed “considerable flexibility” in determining the notion of ‘establishment’. He had observed that this definition is in line with the Court’s case law relating to other fields of EU law.

Taking into account the objective of the data protection rules to protect the fundamental rights and freedoms of natural persons, especially their right to privacy with respect to the processing of personal data, Cruz Villalón stressed that the effective exercise of activities as well as the degree of stability of the arrangements need to be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. Similarly, in Google Spain and Google Advocate General Jääskinen noted that the business model of the company needs to be taken into account when interpreting Article 4 of the DPD. As noted by Cruz Villalón, considering the nature of the economic activities is especially important with undertakings offering services online. In today’s digitalised world the importance of the concept of fixed establishment has diminished. In some circumstances, the presence of a single representative can suffice to be considered as a stable arrangement, if this representative acts with a sufficient degree of

---

137 Case C-230/14 para 66.
138 Opinion of Advocate General Cruz Villalón, case C-230/14, para 28-29; Case C-230/14 para 29.
139 Opinion of Advocate General Cruz Villalón, case C-230/14, para 32.
140 Opinion of Advocate General Jääskinen, case C-131/12, para 65.
141 Opinion of Advocate General Cruz Villalón, case C-230/14, para 34.
stability through the presence of the necessary equipment. For example, the requirements can be met when an agent is permanently present on the territory of the Member State in question and equipped with a laptop. In addition, considering the objective of the DPD, even a minimal activity can be regarded as effective exercise in the sense of the DPD.142

The Court clearly expressed in Weltimmo that some physical presence on the territory of a Member State is required in order to fulfil the conditions of an establishment. A branch or subsidiary is not a requirement, and even a person’s presence can be sufficient if this presence is stable.

By applying e contrario reasoning, if these conditions of effectiveness and permanence (as developed by Cruz Villalón) are not met, it could, in my opinion, be argued that the controller or the processor in question does not have an establishment in the EU. Article 3(1) of the GDPR is therefore not applicable, and the question is whether Article 3(2) of the GDPR can be applied instead.

4.3 Which cross-border situations are covered by the GDPR?
As discussed above, Article 3(2) of the GDPR is applicable when the controller or the processor is not established in the EU and the data subject is physically present in the EU. Hence, the GDPR does not cover all cross-border situations where the controller is established in a third country and the data subject is present in the EU. Article 3(2) of the GDPR requires that one of the two criteria specified in the provision is fulfilled. Article 3(2) states that the GDPR applies to processing of personal data when the processing activities are related to the offering of goods or services to data subjects in the Union or to the monitoring of their behaviour.

It is worth noting that the GDPR applies when the processing activities are related to either offering of goods or services to data subjects in the EU, or to the monitoring of their behaviour. It has been argued that this leads to the application of the Regulation as soon as the activities concern data subjects in the EU.143 Thus, the term ‘related to’ seems,

---

142 Opinion of Advocate General Cruz Villalón, case C-230/14, para 32-34; Case C-230/14 para 29-31.
in my opinion, to be a rather vague notion that does not require any strong connection between the processing activities and the offering of goods or services or the monitoring of the behaviour. This does not, however, cause a problem to arise with the notion of ‘related to’ since it clearly requires that there is a connection between the processing activities on the one hand and the offering of goods or services or monitoring of the behaviour on the other. The two criteria in Article 3(2) further specify when the GDPR is to be applied. These criteria in Article 3(2)(a) and Article 3(2)(b) will be analysed in Chapters 5 and 6.
Offering goods or services to data subjects in the EU

5.1 Identifying the criteria in Article 3(2)(a) of the GDPR

GDPR applies, as mentioned above, to the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union if one of the two conditions in Article 3(2) is met. This section examines the first of these two conditions, namely when the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union.

The provision is explained in recital 23 of the GDPR which states the following:

“In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.”

144 Emphasis added.
5.1.1 Offer of goods or services

The processing activities need to be related to the offering of *goods or services*. There is, however, no definition for the terms ‘goods’ and ‘services’ in the GDPR. A definition of ‘goods’ can be found in the Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights (‘the Consumer Directive’). According to Article 2(3) of the Consumer Directive goods are “any tangible movable items, with the exception of items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity”. Since the GDPR does not exclude any categories of goods or services, it is argued that all types of goods and services should be covered by the GDPR. The provision does mention, as already stated, that the Regulation applies to goods or services that are paid as well as to the ones that are free. Since the Regulation does not expressly exclude any types of goods or services, it should, according to Jay, apply even if the goods or services are not lawful or regulated, and regardless of whether they are offered occasionally or whether they are permanently on offer.\(^{145}\)

The GDPR applies, however, only if some *processing* of personal data takes place. The mere fact that a company is offering goods or services on a website does not automatically mean that the GDPR is to be applied. Nevertheless, in most cases the offering of goods or services includes processing of data due to the use of cookies and routine collection of Internet Protocol (‘IP’) addresses.\(^{146}\) That processing of personal data is required in order to apply Article 3(2) is an obvious criterion since the GDPR regulates the processing of personal data. Yet it is in my opinion necessary to acknowledge that this is a criterion among others in Article 3(2) of the GDPR.

5.1.2 The concept of targeting

That a company which has a website where it offers goods and processes the personal data of the visitors of that website does not automatically mean that the GDPR is to be


applied to the processing. Article 3(2)(a) of the GDPR requires that there is an offer of the goods or the services to data subjects present on the territory of the EU. Firstly, it can be noted that there is no requirement that the data subject buys those goods or uses the services; what is required is that the trader offers goods or services. In my opinion it can also be argued that the fact that a data subject actually buys the goods or uses services is irrelevant for the applicability of Article 3(2)(a) of the GDPR. Recital 23 of the GDPR (cited above) states that in order to determine whether a controller or a processor is offering goods or services to data subjects who are in the Union, it needs to be ascertained whether it is apparent that the controller or the processor envisages offering goods or services to data subjects in the EU.

The criterion of ‘envisaging’ is similar to the criterion of ‘orientating’ business activities to the EU, used and developed by the CJEU in EU case law. 147 Both the criterion of ‘orientating’ and the criterion of ‘envisaging’ are examples of the concept of targeting, which requires an intention to target a certain territory. More precisely, a business activity needs to be intended to have effects within the territory of the state which is asserting jurisdiction. 148 Therefore, the targeting approach requires the identification of the intentions of the parties and to determine the steps taken to either enter or avoid a specific jurisdiction. 149

The use of the concept of targeting is new in EU data protection law. 150 The 29WP has stated that targeting of individuals should be added as an additional criterion to Article 4(1)(c) of the DPD when the controller is not established in the EU. This would, according to the 29WP, ensure a sufficient connection with the EU and would hinder controllers established in third states to use EU territory to conduct illegal data processing activities. 151

As addressed above, the applicability of the DPD is based on an establishment in the EU or alternatively on the use of equipment on the territory of the EU. In the Google Spain

---

148 Schultz, T, Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface, p 817.
149 Geist, M, Is There a There There? Toward Greater Certainty for Internet Jurisdiction, p 1346.
150 See De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.
and Google case the Court interpreted Article 4(1)(a) and stated that processing of personal data is carried out in the context of the activities of the controller on the EU territory when “the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activities towards inhabitants of that Member State.”\(^{152}\) It could be argued that the Court added a new condition to the applicability of Article 4(1)(a) of the DPD, namely the criterion of orientating activities.\(^{153}\)

As Brkan notes, adding a new criterion to Article 4(1)(a) of the DPD that does not appear in the text of the provision is questionable. An addition of the concept of targeting to Article 4(1)(a) can hardly be a result of a textual or teleological interpretation of the notions expressed in the Article.\(^{154}\) On the other hand, the notion of orientating was given by the national court in its preliminary question, and not formulated by the CJEU itself. In the light of this, it could be argued that the Court did not add a new criterion to Article 4(1)(a), but only replied to a question which included a concrete situation as an example.\(^{155}\) Therefore, it is doubtful whether the Court actually created a new criterion in its judgment in the Google Spain and Google case. I support the second alternative, namely that the Court did not create a new criterion but instead answered to a question formulated by the national court. As a consequence, it can be noted that the concept of targeting used in the GDPR is new in the concept of data protection law in the EU. Thus, the interpretation of Article 4 of the DPD does not provide any guidance when interpreting Article 3(2)(a) of the GDPR. However, the concept of targeting is familiar from EU case law regarding other fields of law.

### 5.2 The concept of targeting and EU case law

The concept of targeting has been used in several rulings given by the CJEU in the recent years. The concept is particularly important in the context of trading activities on the internet. The idea behind the use of this concept is on the one hand to prevent that all online activities would be subject to all laws of the countries in which the internet is

---

\(^{152}\) Case C-131/12 para 60.

\(^{153}\) Brkan, M, Data Protection and European Private International Law, p 33.

\(^{154}\) Brkan, M, Data Protection and European Private International Law, p 33.

\(^{155}\) Brkan, M, Data Protection and European Private International Law, p 34.
accessible. One the other hand, the concept of targeting seeks to prevent that a trader escapes from the laws of a country which it is targeting. The concept of targeting is especially used in the context of consumer law and intellectual property law.\textsuperscript{156}

5.2.1 Targeting and consumer contracts

The concept of ‘directing activities’ is used both in the Rome I Regulation and the Brussels I bis Regulation (as well as in the Brussels I Regulation) in the context of consumer law. The EU case law that will be discussed in this Chapter concerns the interpretation of the concept of ‘directing activities’ in Article 15(1)(c) of the Brussels I Regulation but is, as noted in Chapter 1, also relevant for the interpretation of Article 17(1)(c) of the Brussels I bis Regulation.\textsuperscript{157}

Article 17(1)(c) of the Brussels I bis Regulation states that rules on jurisdiction over consumer contracts applies if the professional directs commercial or professional activities to the Member State of the consumer’s domicile. The concept of directing activities can also be found in Article 6 of the Rome I Regulation according to which the law applicable to a consumer contract is the law of the country where the consumer has his or her habitual residence, under the condition that the professional directs his commercial or professional activities to that country.

The GDPR uses the words ‘offering goods or services’ instead of ‘directing activities’. Interestingly, the draft version of the European Commission’s proposal for the GDPR from 2011 (the interservice version)\textsuperscript{158} states, in its Article 2(2), that the Regulation applies – when the controller is not established in the EU – when the processing activities are directed to data subjects residing in the EU or when the processing activities serve to monitor the behaviour of those data subjects.\textsuperscript{159} Even though ‘directing activities’ was replaced by ‘offering goods or services’ in the final version of the GDPR, the drafters of the GDPR must have had in mind the EU regulations and the EU case law where the

\textsuperscript{156} Stone, P, Territorial targeting in EU private law, p 14-15.
\textsuperscript{157} See Stone, P, EU Private International Law, p 22-23.
\textsuperscript{158} The European Commission’s Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Version 56 (draft).
expression of ‘directing activities’ has been used, when drafting the new GDPR and its Article 3(2).

5.2.1.1 Joined cases Pammer and Hotel Alpenhof

The concept of targeting was used by the CJEU in the joined cases Pammer (C-585/08) and Hotel Alpenhof (C-144/09) concerning the interpretation of Article 15(1)(c) of the Brussels I Regulation. The Pammer case was about a dispute between Mr Pammer residing in Austria and a company established in Germany concerning a voyage by freighter. Mr Pammer had booked the voyage through an intermediary company which operated via the internet. Since the description did not correspond to the conditions on the vessel, Mr Pammer claimed payment before an Austrian court. The company had reimbursed only a part of the sum for the voyage.

The Hotel Alpenhof case concerned a dispute between a company (Hotel Alpenhof) operating a hotel (also named Hotel Alpenhof) in Austria and a consumer residing in Germany. The customer had found a hotel on the internet and reserved several rooms in it. However, he had refused to pay for the rooms due to faults in the hotel’s services, despite the offered reduction by the hotel. As a result, the company brought an action before an Austrian court. In both cases, the defendant raised a plea that the court before which the action in question had been brought lacked jurisdiction.

The Austrian Supreme Court was of the view that the two cases, Pammer and Hotel Alpenhof, should be joined due to the similarity of the questions in these cases. Two of the questions referred by the Austrian Supreme Court to the CJEU for a preliminary ruling concerned the interpretation of the criterion ‘directing activities’ in Article 15(1)(c) of the Brussels I Regulation. Regardless of the fact that determining the concept of “directing activities” is no easy task, the CJEU provided some concrete criteria in its ruling. The Court concluded that in order to determine whether a trader is directing its activity to the

---

160 Joined cases C-585/08 and C-144/09, para 14-16.
161 Joined cases C-585/08 and C-144/09, para 17.
162 Joined cases C-585/08 and C-144/09, para 18 and 28.
163 Joined cases C-585/08 and C-144/09, para 32.
164 Joined cases C-585/08 and C-144/09, para 31 and 47.
consumer’s domicile in the EU, “it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader’s overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer’s domicile, in the sense that it was minded to conclude a contract with them.” Furthermore, the Court gave a non-exhaustive list of matters indicating that the activities are directed to a certain territory, such as “the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader’s site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States.”

Stone argues that when it comes to contracts concluded by means of an order placed electronically by a consumer, and via a trader’s website, careful examination is required in order to determine whether the trader was directing activities to the Member State of the consumer’s domicile. Furthermore, Stone notes that in the majority of cases the conclusion is that the business was directing its activities to the country of the consumer’s domicile.

5.2.1.2 The Mühlleitner case and the Emrek case

The joint ruling of the Court in Pammer and Hotel Alpenhof was followed by two subsequent rulings, namely the cases Mühlleitner (C-190/11) and Emrek (C-218/12).\footnote{Joined cases C-585/08 and C-144/09, para 92.} \footnote{Joined cases C-585/08 and C-144/09, para 93.} \footnote{Stone, P, EU Private International Law, p 137-138.} \footnote{Brkan, M, Data Protection and European Private International Law, p 14.}
Both these cases concerned the interpretation of Article 15(1)(c) of the Brussels I Regulation.

The question in the Mühlleitner case was whether Article 15(1)(c) is limited to distance contracts.\(^{170}\) In this particular case, Ms Mühlleitner, domiciled in Austria, had searched for a car of a German make on the internet. After having selected a car on the internet, she was directed to an offer from Mr. A Yusufi and Mr. W Yusufi (the defendants). She contacted the defendants by using the phone number appearing on the website of the seller, and including an international dialling code. Ms Mühlleitner went to Germany and bought the car from the defendants by a contract of sale. Back in Austria, she noticed the car was defective, and asked the defendants to repair the car. The defendants refused to do so, and as a consequence Ms Mühlleitner brought proceedings against the defendants in the court of her place of domicile, for rescission of the contract. The defendants contested the international jurisdiction of Austrian courts, as well as Ms Mühlleitner’s status of ‘consumer’.\(^{171}\)

The Court ruled that Article 15(1)(c) does not require that the contract between a consumer and a trader is concluded at a distance. The Court stated that the provision does not expressly require that the provision would be limited to contracts concluded at a distance. In addition to the wording of the provision, the Court interpreted the provision in the light of its objective by using the method of teleological interpretation. To require that a contract is concluded at a distance would, according to the Court, conflict with the objective of the provision. Such a condition would not be in line in particular with the objective of protecting the consumer as the weaker party to the contract.\(^{172}\) However, the Court noted that factors such as the establishment of a contact at a distance or the reservation of goods or services at a distance indicate that the consumer contract is connected with an activity which is directed to the Member State of the consumer’s domicile.\(^{173}\)

In the Emrek case, the question was whether Article 15(1)(c) required that the consumer was encouraged by the website of the trader to conclude the contract, and whether there,

\(^{170}\) Case C-190/11 para 24.
\(^{171}\) Case C-190/11 para 11-17.
\(^{172}\) Case C-190/11 para 33-45.
\(^{173}\) Case C-190/11 para 44.
as a consequence, needed to be a causal link between the website and the conclusion of the contract. Mr Emrek, domiciled in Germany, had been looking for a second-hand vehicle. The defendant, Mr Sabranovic, operated a business selling second-hand motor vehicles in France. Mr Sabranovic had a website containing contact details to his business which included French telephone numbers as well as a German number, both with the international codes. Mr Emrek learned about Mr Sabranovic’s business from acquaintances and went to the business premises in France and concluded a contract for the sale of a second-hand vehicle. Later on, Mr Emrek brought proceedings against the defendant in the local court of Saarbrücken where he had his domicile.\textsuperscript{174}

The Court found that Article 15(1)(c) of the Brussels I Regulation does not require a causal link between the website used to direct the commercial activities to the Member State of the consumer’s domicile on the one hand, and the conclusion of the consumer contract on the other. The Court noted that the provision in question does not expressly require the existence of such a causal link. Adding an unwritten condition to Article 15(1)(c) would in the Court’s view be contrary to the objective of the provision, namely to protect consumers who are considered as weaker parties in relation to traders. As in the \textit{Mühlleitner} case, the Court started with the literal interpretation and continued with the teleological interpretation.\textsuperscript{175}

Furthermore, the Court argued that despite the fact that there is no requirement for a causal link in Article 15(1)(c) of the Brussels I Regulation, such a causal link may constitute strong evidence which may be considered by the national courts when determining whether the trader’s activities are directed to the Member State of the consumer’s domicile. The Court referred to the non-exhaustive list given by the Court in the \textit{Pammer and Hotel Alpenhof} case, as well as to the conclusions of the Court in the \textit{Mühlleitner} case. In the \textit{Mühlleitner} case, the Court had added some factors, such as the ‘establishment of contact at a distance’, to the non-exhaustive list developed in \textit{Pammer and Hotel Alpenhof}. These factors may constitute evidence for a connection between the contract and the directed activity.\textsuperscript{176}

\textsuperscript{174} Case C-218/12 para 9-13.  
\textsuperscript{175} Case C-218/12 para 21-24 and 32.  
\textsuperscript{176} Case C-218/12 para 20-32.
Finally, it can be noted that in both the *Mühlleitner* case and the *Emrek* case the Court underlines that the essential criterion in Article 15(1)(c) of the Brussels I Regulation is that a commercial or a professional activity is directed to the Member State of the consumer’s domicile.\footnote{Case C-190/11 para 44; Case C-218/12 para 23.}

5.2.2 Targeting in the field of intellectual property rights

5.2.2.1 *The case of L’Oréal and Others*

The targeting approach can also be found in the case law of the CJEU in the context of intellectual property rights. The first of these judgments is the case of *L’Oréal and Others* (C-324/09). In this particular case, trademarks registered in the EU had been put on sale by an economic operator in a third country, on an online marketplace, and without the consent of the trademark proprietor. The relevant question for this study concerned the interpretation of Article 5 in the First Council Directive 89/104/EEC of 21 December 1988 to approximate the Laws of the Member States relating to Trade Marks\footnote{OJ L 40/1.} and Article 9 of the Council Regulation (EC) No 40/94 of 20 December 1993 on the Community Trade Mark.\footnote{OJ L 11/1.} The Court ruled that the trademark proprietor has the right to prevent the sale, offer for sale or advertising of goods when these goods are offered for sale or advertised on an online marketplace targeted at consumers located in the EU.\footnote{Case C-324/09 para 67.}

Furthermore, the Court noted that the assessment whether the offer for sale is targeted at consumers in the EU must be done on a case-by-case bases. However, factors such as details of the geographic areas to which the seller intends to dispatch its product are of particular importance.\footnote{Case C-324/09 para 65.} It also added that the accessibility from the territory covered by the trademark is insufficient, and referred to *Pammer and Hotel Alpenhof* (para 69) where the Court ruled that the mere accessibility of the trader’s website is insufficient to conclude that the trader is directing its activities to the consumer’s domicile.\footnote{Case C-324/09 para 64. See also joined cases C-585/08 and C-144/09, para 94.}
The Court arrived at its conclusion by stating that if operators targeting consumers in the EU through an online marketplace would not need to comply with the EU intellectual property rules due to the fact that the goods are located in a third country, the effectiveness (effet utile) of these EU rules would be undermined. The Court referred to the opinion of Advocate General Jääskinen who had noted that if EU law would not be applicable in the cases mentioned by the Court, companies could escape EU law by situating the activity or the website in a third country. The ruling of the Court together with the opinion of Advocate General Jääskinen give support to the statement that the application of EU law cannot be limited solely to situations where the goods are put on market in the EU.183

5.2.2.2 The case of Football Dataco and Others

The case of Football Dataco and Others (C-173/11) concerned the interpretation of Article 7 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases.184 According to this provision, EU Member States shall provide a right for the maker of a database to prevent extraction and/or re-utilisation of the contents of that database (a sui generis right). The circumstances in the case were the following. Football Dataco and Others (the plaintiffs), were responsible for organising football competitions in England and Scotland and had a database called ‘Football Live’ which contained data on the football matches. They claimed to have a sui generis right to the database. Sportradar GmbH (the defendant) was a German company providing results and statistics about inter alia English league matches live and via the internet. Football Dataco and Others brought proceedings against Sportradar in the High Court of Justice of England and Wales. The plaintiffs sought compensation for the damage relating to an infringement by Sportradar of their sui generis right. The plaintiffs claimed that Sportradar had obtained its data by copying that data from Football Live onto its server, and that the copied data was then transmitted to the public in the United Kingdom (‘UK’).185 According to Article 5(3) of the Brussels I Regulation, the competent

---

183 Opinion of Advocate General Jääskinen, case C-324/09, para 127; Case C-324/09 para 62-63.
185 Case C-173/11 para 8-15.
courts in matters related to tort, delict, and quasi-delict are the courts for the place where “the harmful event occurred or may occur”.

The Court found that Article 7 of the Directive 96/9 must be interpreted as meaning that the sending by one person, by means of a web server located in Member State A, of data that had previously been uploaded by that person from a database protected by the sui generis right under the Directive 96/9 to the computer of another person present in Member State B, at that person’s request, for the purpose of storage in the computer’s memory and display on its screen, constitutes an act of ‘re-utilisation’ of the data by the person sending it. Furthermore, the Court ruled that this act of re-utilisation of the data takes place, at least, in Member State B, under the condition that there is evidence supporting that the person performing the act had an intention to target members of the public in Member State B.\textsuperscript{186}

The Court noted that the sui generis right is, in principle, limited to the territory of the Member State that provides the right in question, and it only protects against acts of re-utilisation which take place within that territory. It is therefore relevant to know whether an act falls within the territorial scope of the protection by the sui generis right.\textsuperscript{187} The Court referred to the joint ruling in Pammer and Hotel Alpenhof as well as to the ruling in L’Oréal and Others when it stated that the mere accessibility of the website is not sufficient for concluding that the act of re-utilisation took place in the territory of the UK. The location of an act of re-utilisation in the territory of the Member State to which the data was sent depends, according to the Court, on there being evidence from which it may be concluded that the performer of the act had an intention to target persons present within that territory.\textsuperscript{188}

For example, that fact that the data on the defendant’s server included data concerning English football matches could constitute such evidence. Also, that Sportradar had concluded contracts concerning the right to access Sportradar’s servers, with betting companies which offered betting services to the public in the United Kingdom, could constitute evidence. In order to be considered as evidence, the Court required that

\textsuperscript{186} Case C-173/11 para 47.
\textsuperscript{187} Case C-173/11 para 27-28.
\textsuperscript{188} Case C-173/11 para 36-39.
Sportradar was aware, or must have been aware, of the destination. Finally, the fact that the defendant’s website was accessible to users in the United Kingdom in their own language, other than the language commonly used in the Member State from which the defendant was pursuing its activities, could be considered as supporting evidence.\textsuperscript{189}

As Stone notes, the Court focused on the territorial scope of the \textit{sui generis} right under the Directive 96/9 and not on Article 5(3) of the Brussels I Regulation which was the basis of the jurisdiction of the referring court.\textsuperscript{190} This may, in my opinion, be due to the question referred to the CJEU which was focused on the \textit{sui generis} right under the Directive 96/9. Thus, it is in my view not surprising that the Court did not have its focus on Article 5(3) of the Brussels I Regulation.

Furthermore, it is worth noting that what the \textit{Dataco and Others} case and the GDPR have in common is that the concept of targeting is used in order to determine the territorial scope of application of a provision.

5.3 Interpretation of Article 3(2)(a) in the light of EU case law

5.3.1 The targeting approach and \textit{effet utile}

The use of the concept of targeting is motivated by the argument concerning the effectiveness of EU law. As Advocate General Jääskinen and the Court noted in the \textit{L’Oréal and Others} case, the effectiveness, or \textit{effet utile}, of EU law would not be guaranteed if companies established outside the EU and targeting the consumers in the EU would not need to comply with the EU rules concerning consumer protection, protection of intellectual property rights and other fields of law.\textsuperscript{191}

The same can be argued about EU data protection law and the protection of data subjects present in the EU. If targeting of data subjects in the EU would not be sufficient to apply the GDPR, a company could escape the relatively strict rules of GDPR by moving its establishment and equipment to a third country. This has been identified as a problem with the criterion ‘use of equipment’ in the DPD, as it requires physical presence in the

\textsuperscript{189} Case C-173/11 para 40-42.
\textsuperscript{190} Stone, P, Territorial targeting in EU private law, p 22.
\textsuperscript{191} Opinion of Advocate General Jääskinen, case C-324/09, para 127; Case C-324/09 para 62-63.
EU. The DPD does not cover the cases where personal data is processed by a controller without any physical presence in the EU, but which targets data subjects in the EU.\textsuperscript{192}

Furthermore, many of the controllers and the processors processing personal data of data subjects present in the EU are companies that are established outside the EU. If the GDPR would not apply to these companies located in third countries, the GDPR would provide weak protection to the data subjects in the EU. In order to guarantee the effectiveness of the Regulation, it is necessary that it applies to companies established in the EU, as well as companies established outside the territory of the EU.

5.3.2 Accessibility of a website – not a sufficient factor
It is clear from recital 23 that in determining whether goods or services are offered to data subjects in the EU, it is not sufficient that these data subjects have access to the offer on a website. Thus, it can be noted that the GDPR is well in line with the rulings in \textit{Pammer and Hotel Alpenhof} and the other cases discussed above since in these cases the mere accessibility of a website was an insufficient factor to consider that a business was targeting consumers in an EU Member State. In the \textit{L’Oréal and Others} case, the Court noted that if accessibility would be sufficient, third country companies that are only targeting consumers in a third state would wrongly need to comply with EU law.\textsuperscript{193}

The GDPR is also in accordance with CJEU’s reasoning in the \textit{Bodil Lindqvist} case. In this preliminary ruling, the CJEU answered to several questions, one of them being particularly relevant for this study. The Court stated that the mere fact that data was published on the internet and accessible also in third countries does not necessarily mean that there has been a transfer of data to a third country, within the meaning of Article 25 of the DPD. The Court noted that the legislator could not have meant that Article 25 of the DPD would apply every time data was uploaded on the internet and made accessible in all the third countries having the technical means to access the internet. Such an interpretation would result in the DPD having general application regarding operations

\textsuperscript{192} See Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, p 43-44.

\textsuperscript{193} Case C-324/09 para 64.
on the internet.\textsuperscript{194} In this way, as Kuner notes, the Court denied that EU data protection law would apply to the entire internet. The EU data protection rules should therefore not be interpreted as having universal application.\textsuperscript{195}

Furthermore, Advocate General Jääskinen noted in his opinion concerning the Google Spain and Google case that the Court rejected, in the Bodil Lindqvist case, an interpretation of the DPD that would lead to an unreasonably wide scope of application of Article 25 of the DPD. Accordingly, the Court applied the principle of proportionality in order to avoid unreasonable and excessive legal consequences.\textsuperscript{196} Concerning the Google Spain and Google case, Jääskinen argued that it was “necessary to strike a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and internet users at large.”\textsuperscript{197} It is, in my view, important to strike this balance also when interpreting and applying the GDPR. The territorial scope of application of Article 3(2) of the GDPR should not extend further than what is reasonable and proportionate. To apply the GDPR to all websites accessible from the EU would, in my view, be neither proportionate nor reasonable. There should be a sufficient connection between the business activities and the territory where the data subjects are present. The concept of targeting is one way to define the territorial scope of a provision and to determine when there is a sufficient connection between an activity and a territory. In the context of EU data protection law, the targeting approach requires that the business has an intention to target data subjects in the EU.

5.3.3 Intention to target

After having discussed some of the preliminary rulings where the CJEU has used the concept of targeting, many similarities with the GDPR can be found in these rulings. Most notably, the joint ruling in Pammer and Hotel Alpenhof is relevant in order to define the territorial scope of the GDPR.

\textsuperscript{194} Case C-101/01 para 68-69.
\textsuperscript{195} Kuner, C, Extraterritoriality and regulation of international data transfers in EU data protection law, p 242.
\textsuperscript{196} Opinion of Advocate General Jääskinen, case C-131/12, para 30.
\textsuperscript{197} Opinion of Advocate General Jääskinen, case C-131/12, para 31.
The non-exhaustive list given by the CJEU in *Pammer and Hotel Alpenhof* is much longer than the one in recital 23 of the GDPR. Nevertheless, several matters listed by the Court are also found in recital 23, such as the use of language or currency generally used in one or more Member States and the mentioning of customers in the EU. Also the wording is similar since both in the Court’s reasoning and in recital 23 of the GDPR the keyword is *envisaging*. The resemblance is apparent and Article 3(2) was certainly inspired by the conclusions of the Court in *Pammer and Hotel Alpenhof*. Therefore, it can be assumed that even the factors mentioned in the case but which do not appear in recital 23 will probably be useful evidence in data protection disputes. Also in *L’Oréal and Others*, the Court stated that relevant factors such as details of the geographic areas to which the seller is willing to offer the product are of particular importance. Both cases, as well as the three other cases discussed above, provide with concrete factors that could, in my view, also be relevant in order to determine whether goods or services are offered to data subjects in the EU.

The concept of targeting developed in the *Pammer and Hotel Alpenhof* case, as well as in the cases *L’Oréal and Others* and *Football Dataco and Others* seems to focus on the subjective intention of the defendant to direct its activities to a certain state territory. The subjective intention is proved by objective criteria such as the factors mentioned in the non-exhaustive list in *Pammer and Hotel Alpenhof*. Svantesson criticises the reasoning of the Court in *Pammer and Hotel Alpenhof* because it focuses on the subjective intentions of a business. Svantesson notes that CJEU seems to have interpreted the notion of ‘directing activities’ as implying “a conscious decision executed without mistakes”. The Court’s view was fully in line with the opinion of Advocate General Trstenjak who stated that the notion ‘directing activities’ requires that the undertaking actively endeavours to conclude contracts with consumers in the EU. In addition, she noted that: “It is therefore essential for there to be active conduct on the part of the undertaking, the objective and outcome of which is to win customers from other Member States.” Svantesson does not agree with this statement of the Advocate General since both the objective and the outcome are given importance. In Svantesson’s view a better approach

---

199 Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, p 232.
200 Opinion of Advocate General Trstenjak, joined cases C-585/08 and C-144/09, para 63.
would be to distinguish these two terms and only focus on the outcome in order to
determine whether the business directed its activities to the consumer in the EU. This
would, according to Svantesson, promote certainty and fairness.\(^{201}\)

I partly agree with Svantesson. Firstly, in my view Svantesson’s argument about
distinguishing between the objective and the outcome appears reasonable. My
interpretation of the Court’s reasoning in *Pammer and Hotel Alpenhof* as well as the
wording in Article 3(2)(a) is that the *objective* of the business to target consumers in the
EU is essential. That the intention to target is the essential condition is expressly stated
by the CJEU in its case law.\(^{202}\) The focus is on the subjective intention of the business,
and not on the outcome. The decisive factor should therefore be the objective of the
business.

Another important point to consider is, however, whether it is in practice possible to
determine whether a company established outside the EU intends to target data subjects
in the EU. An illustrative example of a company that probably falls within the scope of
Article 3(2)(a) of the GDPR is the camera company Snap Inc. and its product called
Snapchat.\(^{203}\) This is the case if the personal data of data subjects in the EU is not processed
in the context of the activities of an establishment in the EU. Consider that the company
is not established in the EU and the personal data of data subjects in the EU is processed
in the context of the activities of the establishment of Snap Inc. in the US.

By using Snapchat, individuals can send each other pictures (‘Snaps’) or videos that
disappear after some seconds. When visiting the website\(^{204}\) of the company, the website
recognises the country where the person visiting the website is present, and automatically
chooses the language spoken in that country. For example, if one visits the website from
Sweden, the website will automatically appear in Swedish. There are several language
options on the website and the company has different Terms of Service for the users living

\(^{201}\) Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the
regulation, p 232.
\(^{202}\) See case C-190/11 para 44; Case C-218/12 para 23.
\(^{203}\) Murray, A, Information Technology Law: The Law and Society, p 582.
\(^{204}\) https://www.snap.com/en-GB/
in the US on the one hand and the users living outside the US on the other. It is therefore clear that the company targets users outside the US.\footnote{https://www.snap.com/en-US/terms/}

There are surely also cases where it is difficult to determine whether the GDPR applies or not. If none of the factors mentioned in the GDPR or in the rulings in the cases discussed above are present on the website of a company, is it still possible that the GDPR applies to that company? The following imaginary example illustrates the problem with the criteria given in the GDPR. A Canadian yoga studio gives yoga lectures in Québec. In order to participate in their yoga classes, the participants need to register on the website of the company and book classes online. I decide to leave my university town Uppsala for a month and visit a friend in the French speaking Québec. I decide to do some yoga there so I register on the website of the yoga studio. I fill in my name, e-mail address, date of birth and gender. The website is in French and in English and there is nothing on the website that would indicate that the studio would target the EU. In the coming days I receive e-mails advertising different yoga classes in different countries including Canada and Europe. Does the GDPR apply to this case? According to recital 24, the answer should be negative since there are no factors indicating that the company has a subjective intention to target persons in the EU.

An extensive interpretation could result in considering that the website targets the whole world, including the EU, since it does not clearly appear from the website that the company is solely targeting individuals present in Canada. An extensive interpretation could be supported by a teleological interpretation. As noted above, the CJEU seems to interpret the scope of the territorial application of EU data protection law rather broadly, and in the light of the objective to protect data subjects in the EU. Such an extensive interpretation would in my view be against the wording in Article 3(2) of the GDPR, since the provision requires that a business has an intention to target a specific state territory. The issue of targeting the entire world will be discussed in the following section.
5.3.4 Targeting the entire world

In today’s globalised world it is not unusual for businesses being or seeking to become global actors. That a business acts globally does not necessarily mean that the business targets data subjects in the EU. The question is whether the GDPR is to be applied to these global actors. For example, does the GDPR apply to US companies acting globally, but without specifically targeting the EU?\textsuperscript{206}

Svantesson argues that in many cases there will be a lack of reference to factors stated in recital 23 of the GDPR and indicating that a business is targeting data subjects in the EU. Svantesson stresses that: “courts are going to have to conclude either that [businesses] target just about every country in the world or no countries at all”.\textsuperscript{207}

Additionally, Kuner criticises the EU data protection rules for applying in a black and white fashion. Kuner notes that EU data protection law continues to apply even when the data is transferred outside the borders of the EU, which results in conflicts with the laws of the third countries to which data is exported.\textsuperscript{208} I agree with Kuner that expanding the ‘arm’ of EU data protection law far outside the EU leads to a conflict where the laws of another state equally have a claim for application. The companies may need to apply several laws to their activities if they are willing to be global actors.

On the other hand, if the GDPR is not applicable to the businesses that are targeting everyone, the fundamental right to data protection may not be effectively protected. Applying the GDPR to globally operating companies established in third countries is, in my view, justified as long as there is a fair balance between different interests, such as the protection of personal data of data subjects and legitimate interests of the business. The long arm of the GDPR should, in my opinion, not extend further than what is proportionate and necessary in order to protect data subjects in the EU.\textsuperscript{209}

However, if the GDPR is to be applied in those cases where the company is targeting the whole world, this should be clearly expressed in the GDPR. As already noted, the CJEU

\textsuperscript{206} De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory, p 239.
\textsuperscript{207} Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, p 232.
\textsuperscript{208} Kuner, C, Extraterritoriality and regulation of international data transfers in EU data protection law, 241-242.
\textsuperscript{209} See Opinion of Advocate General Jääskinen, case C-131/12, para 30-31.
has made it clear that the EU data protection law does not apply to the entire internet. Instead, the GDPR is to be applied when the business is targeting data subjects in the EU. The GDPR gives concrete criteria when the business is considered to have a subjective intention to target data subjects present in the EU. In my view it needs to be highlighted that the notion of targeting is a loaded notion which obviously requires an intention to target. Hence, if the Regulation is applied to companies that are not particularly targeting the EU, the result is in my opinion that the GDPR becomes applicable to all global actors who are processing the personal data of data subjects in the EU. This would mean that the factors listed in recital 23 would lose their function since the GDPR would apply regardless of whether such factors are present in a particular case or not. In other words, the GDPR would be applicable despite the fact that a business is not specifically targeting data subjects in the EU.

There is a risk that the GDPR will have a broader territorial scope than what Article 3(2)(a) of the GDPR implies. As a result, the territorial scope of the GDPR becomes unpredictable and legal certainty can no longer be guaranteed. Furthermore, the criterion ‘offering goods or services to data subjects in the EU’ in Article 3(2)(a) may become a vague connection to the EU in cross-border situations. This uncertainty undermines the territorial scope of the GDPR and may weaken the protection of personal data of data subjects in the EU provided in the GDPR. Unawareness among data subjects as well as controllers and processor of which law applies to the processing of personal data would be an undesired consequence.

5.4 Data subject in a contractual relationship
5.4.1 Data subjects as consumers
One could argue that since consumer law (or another field of law) and data protection law are two different fields of laws, it needs to be carefully considered whether it is reasonable to use the criteria developed in the context of consumer rights also in data protection law. Consumer law and data protection law can be treated alike since both data subjects

---

210 Svantesson argues that “drawing upon legal solutions from other fields is sensible, and consumer protection law shares several key features with data privacy law.” See Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, p 231.
and consumers can be considered as weaker parties. In addition, data subjects are sometimes also consumers. The 29WP notes that since the concept of targeting is used in relation to consumer protection, using the concept in the field of data protection would provide additional legal certainty since controllers “would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules”. A data subject can be qualified as a consumer within the meaning of the Brussels I bis Regulation. This is because a data subject is a natural person who can conclude a consumer contract. However, a data subject being a natural person is not automatically considered to be a consumer, since it is also required that this data subject has concluded a contract, and in addition “for a purpose which can be regarded as being outside his trade or profession”.

A difference between consumers and data subjects is that instead of paying for the online services, the users ‘pay’ for the services with their personal data. The data has therefore replaced money as a form of payment in many cases. This has also been taken into account in Article 3(2)(a) which states that the GDPR applies irrespective of whether a payment of the data subject is required. There is also no requirement in the GDPR for a contract between the data subject and the controller. Many service providers such as Google do not have a contract with the users of the search engine. However, other online service providers such as Facebook are in a contractual relationship with their users. The contract between Facebook and its users enables Facebook to include privacy policies within its Terms of Service. According to § 15 of the Terms of Facebook, the laws of the State of California is the applicable law to any claim that might arise between Facebook and its users, regardless of the otherwise applicable conflict of law provisions in a state.

---

211 Rauhofer, J, One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework, p 21.
214 Article 16(1) of the Brussels I bis Regulation.
216 Lipton, J, Rethinking Cyberlaw: A New Vision for Internet Law, p 142-143.
5.4.2 The GDPR in relation to the Rome I Regulation

Facebook is established in the EU and is thus not subject to Article 3(2) of the GDPR. Yet, Facebook and its users is a good example of a contractual relationship between a business and a data subject. The question concerning the possibility for the parties to choose the applicable law to their contract in accordance with the Rome I Regulation is relevant regardless of the location of a controller’s establishment. Before discussing the freedom of choice in Article 3 of the Rome I Regulation, it is worth highlighting that the Rome I Regulation has universal application in all EU Member States. Article 2 of the Rome I Regulation states that any law is to be applied regardless of whether or not it is the law of a Member State. Therefore, the applicable law chosen by the parties can be the law of a third state.

According to Article 3 of the Rome I Regulation the parties have the freedom to choose the applicable law governing their contract. Furthermore, Article 6 of the Rome I Regulation states that the applicable law to consumer contracts is the law of the country where the consumer has his or her habitual residence. The parties may also choose the applicable law to their consumer contract. Nevertheless, this choice cannot deprive the consumer of the protection afforded to him or her by the law of the country where the consumer has his or her habitual residence (Article 6(2) of the Rome I Regulation). This is due to the fact that a consumer is, as noted above, considered as a weaker party in relation to the business. Recital 23 of the Rome I Regulation states that the weaker parties should be protected by conflict-of-law rules which are more favourable to their interests compared to the general rules.

As stated above, the nature of the relationship between the users and online service providers is similar to the one between consumers and businesses. When the parties enter into a contractual relationship, there is an imbalance between the parties in both of these cases. There is a risk that the weaker party, being a data subject or a consumer, is forced to transact according to the contract that is mostly benefiting the online service provider or the business. If the data subject and the controller could agree on applicable law to

---

218 See recital 18 of the Brussels I bis Regulation; Recital 25 of the Rome I Regulation.
their contract, the companies could easily escape the rules of the GDPR. This would not be in accordance with the objective of the Regulation to protect the data subject.

Another argument for giving priority to the GDPR in relation to the Rome I Regulation is to consider the GDPR as *lex specialis* in relation to the Rome I Regulation. Article 23 of the Rome I Regulation states that the Rome I Regulation does not “prejudice the application of provisions of Community law, which in relation to particular matters, lay down conflict-of-law rules relating to contractual obligations”. Article 3(2) of the GDPR could be considered as a special provision since the provision regulates data protection matters and defines when EU data protection law is applicable. However, it can be questioned whether the provision on the territorial scope of the GDPR can be seen as a conflict-of-law rule. In my view it is possible since Article 3(2) defines when the GDPR is to be applied in cross-border situations, when the data subject is physically present in the EU and the controller has its establishment in a third country. In other words, Article 3(2) functions as a conflict-of-law rule since it determines when the GDPR is the applicable law in cross-border situations.

### 5.4.2.1 Article 3(2) of the GDPR – an overriding mandatory provision?

The rules in the GDPR could potentially be considered as overriding mandatory provisions, according to Article 9 of the Rome I Regulation. The current doctrine is divided concerning the potential mandatory nature of EU data protection law. It could be argued that the EU case law, such as the *Ingmar* (C-381/98) case, confirms that not solely provisions in EU Member States’ law but also provisions of EU law can be qualified as overriding mandatory provisions.

The circumstances in the *Ingmar* case were the following. Ingmar GB Ltd (‘Ingmar’), a company established in the UK, had concluded an agency contract with Eaton Leonard Technologies Inc. (‘Eaton’), a company established in California. According to the contract, Ingmar was appointed as Eaton’s commercial agent in the United Kingdom. The contract included a clause according to which the contract was governed by the law of the state of California. Ingmar brought proceedings against Eaton before the High Court.

---

of Justice of England and Wales and sought payment of commission as well as compensation for damage suffered due to the termination of its relations with Eaton, in accordance with the Commercial Agents Regulations 1993 (referred to as ‘Regulations’), national law of the UK implementing the Council Directive 86/653/EEC of 18 December 1986 on the Coordination of the Laws of the Member States relating to Self-Employed Commercial Agents. The High Court ruled that the ‘Regulations’ were not applicable since the contract was governed by Californian law. Ingmar appealed against the judgment to the Court of Appeal of England and Wales. The Court of Appeal referred for preliminary ruling the question whether Articles 17 and 18 of the Directive 86/653/EEC, which provide certain rights to commercial agents after the termination of agency contracts, applied although the principal was established outside the European Economic Community and the parties had chosen the law applicable to their contract.222

The Court’s answer to the question was that Articles 17 and 18 of the Directive 86/653/EEC must be applied. The CJEU stated that the purpose of Articles 17 to 19 of the Directive 86/653/EEC was in particular to protect the commercial agent after the termination of the contract. The Court further ruled that the rules established for that purpose are mandatory in nature. According to the Court it is essential for the Community legal order that a principal established outside the Community, but whose commercial agent carried on his activity within the Community, cannot evade the provisions of the Directive in question by a choice-of-law clause. The purpose served by the provisions requires that they are applied when the situation is closely linked to the Community, especially where the commercial agent carried on his activity within a territory of a Member State, and irrespective of the law chosen by the parties to govern their contract.223

Bogdan argues that by interpreting the Directive 86/653/EEC, the Court achieved the same result as what applies to consumer contracts according to certain directives in the field of consumer law. The mandatory rules protecting the consumer cannot be derogated from by agreement according to which the law of a third state governs the contract, when the legal relationship has a certain connection with the EU. Furthermore, Bogdan is of the view that the Court’s ruling in the case of Ingmar could be relevant also regarding other

222 Case C-381/98 para 2, 8 and 10-14.
223 Case C-381/98 para 21-26.
EU rules than those concerning commercial agents. Jänterä-Jareborg agrees with Bogdan and notes that the same reasoning, as in the ruling of the Court in the *Ingmar* case, seems to apply to all mandatory rules of EU directives, in particular when a situation involves a weaker party and when the competition within the internal market is at stake. Jänterä-Jareborg states that in situations regarding EU mandatory rules protecting a weaker party and where there is a close connection to the EU the presumption is that these rules are considered as overriding mandatory rules.

In my view, the reasoning and arguments above could be applied in the context of EU data protection law. In order to effectively protect the data subjects in the EU and their personal data, it should not be possible for the parties to escape the rules of the GDPR by choosing an applicable law, other than the GDPR, to govern their contract. The GDPR would provide a weak protection to the data subjects if it was possible to avoid the rules of the Regulation by simply agreeing on the applicable law. The issue concerning data subjects in contractual relations with controllers is also relevant for the topic of the next Chapter, which examines Article 3(2)(b) of the GDPR.

---


6 Monitoring the behaviour of data subjects in the EU

6.1 The notion of monitoring

The GDPR is also applicable to the processing of personal data of data subjects who are in the EU by a controller or a processor not established in the EU, where the processing activities are related to the monitoring of the behaviour of those data subjects as far as their behaviour takes place within the EU, as expressed in Article 3(2)(b) GDPR. The term ‘monitoring’ is not defined in the GDPR. The same term is used in Articles 35(3)(c) and 37(1)(b) of the GDPR. The former provision refers to ‘systematic monitoring’ while the latter refers to ‘regular and systematic monitoring’. However, as the 29WP notes, there is a difference between ‘regular and systematic monitoring’ and ‘monitoring of the behaviour’, and therefore they can be considered as two different notions.226 The GDPR does not define the notion ‘regular and systematic monitoring’ either.

The meaning of Article 3(2)(b) is explained in recital 24 of the Regulation which states the following:227

“The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”

As stated in recital 24, the processing of personal data by a controller or a processor who, on the internet, tracks data subjects in the EU and uses personal data processing techniques falls within the scope of the GDPR. The key question here is whether the controller, established in a third country, is profiling a natural person who is in the Union.

227 Emphasis added.
6.2 Online tracking of data subjects

While the term ‘monitoring’ is not defined in the GDPR, the term ‘profiling’ is. The notion of profiling is defined in Article 4(4) of the GDPR, according to which profiling consists of “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

According to the 29WP it is clear from recital 24 that the notion of ‘monitoring’ includes all forms of tracking and profiling on the internet, including behavioural advertising. It also notes that ‘monitoring’ is not restricted to the online environment, online tracking only being one type of monitoring of the behaviour.228 However, online tracking seems to be one of the reasons, if not even the main reason, for this considerable change from ‘use of equipment’ to ‘monitoring of behaviour’ in determining the territorial scope of EU data protection law.229

An illustrating example of online tracking is the following. I decide to buy shoes online so I visit a website of a company established in the US and selling clothes and shoes online. I try to find a nice pair of shoes for the summer on that website. Some days later I visit again the same website, but this time the website suggests me the kind of shoes I was looking at earlier. The conclusion that can be made is that the website had recorded my behaviour on the website and adapted the content after my interests.230 I am physically present within EU territory and the company is established in a third country. In addition, the website is obviously profiling my behaviour. As a consequence, it can be argued that the GDPR should be applicable in this situation.

Article 3(2)(b) of the GDPR applies to cross-border situations when the controller or the processor is not established in the EU. In these situations, it is mainly the online tracking

that will come into question. The organisations conducting online tracking are often companies that are established outside the territory of the EU. These companies monitoring the behaviour of data subjects in the EU can escape the EU data protection rules under the current legislation since it can be difficult to demonstrate that a company uses equipment in the EU.\textsuperscript{231} It is worth noting that the term ‘profiling’ does not appear in the DPD. The DPD has not been able to provide data subjects a sufficient level of protection for their personal data. Thus, the GDPR and especially its Article 3(2) is a clear response to the technical developments that are challenging the data protection legislation.\textsuperscript{232}

Despite the fact that the DPD does not expressly mention the notions ‘monitoring’ or ‘profiling’, it does include the use of online tracking techniques such as cookies and JavaScript. A cookie is a text file which is placed by the website on the user’s personal computer. Information about the user is stored on the cookie. In case of further communication, the cookie enables the controller to identify the computer and the user. The controller can link up all information about a person, collected during different sessions. As a result, the controller can create a detailed profile of that person. JavaScripts are software applications which the website sends to the user’s computer. They can be used to introduce viruses in the computer, display information on a website, as well as to process personal data stored in the user’s computer. The use of these techniques are considered as ‘use of equipment’ in the sense of Article 4(1)(c) of the DPD.\textsuperscript{233}

Moerel questions the application of Article 4(1)(c) of the DPD whenever cookies or other ‘tools’ are used, since it results in the application of the protection principle, instead of the territoriality principle. According to the protection principle, the connecting factor is the location of the persons to be protected, and the relevant factor is the action of the actor; in the context of EU data protection, the location of the data subject in the EU is


\textsuperscript{233} Article 29 Data Protection 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 websites, p 10 ff; Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, p 39.
the determining factor. Moerel argues that this is not in accordance with the choice of the legislator, since Article 4(1)(c) is based on territoriality principle. According to the territoriality principle, the connecting factor is the location of the actor, namely the location of the controller and its equipment.234

I agree with Moerel that the application of the protecting principle in the context of Article 4(1)(c) of the DPD is not in line with the wording of the provision. If the location of the data subject is the determining factor, it should also be expressed in Article 4(1)(c). As the provision is currently formulated, the DPD applies when the equipment is located in the EU. Therefore, the location of the equipment and not the location of the data subject is decisive whether the DPD is applied or not. Thus, considering the location of the data subject as the connecting factor is against the wording of the provision. In my view, such an interpretation results in uncertainty concerning the territorial scope of the DPD and therefore threatens legal certainty.

Concerning Article 4(1)(c), the 29WP has also stated that it would “advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.”235 Moerel argues that this statement is vague and that the factors mentioned by the 29WP are not based on Article 4(1)(c) of the DPD. She notes that despite the good intention of the 29WP to provide protection to data subjects in the EU, this should be done by the legislator, and by bringing the applicability rule in line with the general rules of private international law.236 Again, I agree with Moerel. In order to guarantee predictability and legal certainty to data subjects as well as controllers and processors, it needs to clearly appear from the provision which situations are within the scope of the DPD.

235 Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU web sites, p 9.
The wording in Article 3(2)(b) of the GDPR is a big improvement compared to Article 4(1)(c) of the DPD. Both the GDPR and the DPD seeks to cover online tracking, but only the GDPR expressly includes online tracking within the scope of the Regulation. However, it can be noted that this has mainly to do with the fact that the DPD was drafted in 1995, and since that time technology has taken a considerable step forward. It is definitely time to amend the relevant legislation, so that it can adequately respond to the challenges posed by the fast developing technology.

6.3 Processing of personal data
Common between the DPD and the GDPR is that only processing of personal data is covered. Therefore, the qualification of the data as personal data is a decisive factor when it comes to the applicability of the DPD and the GDPR. In Article 4(1) of the GDPR and in Article 2(a) of the DPD, personal data is defined as any information relating to an identified or identifiable natural person. Anonymous information, namely information that is not related to an identified or identifiable natural person, falls outside the scope of the GDPR. Similarly, the GDPR does not apply to information that is rendered anonymous in a manner that the person is no longer identifiable.

The 29WP notes that a natural person in a group is identified when the person is distinguished from other members of the group. A person can be either directly or indirectly identifiable. A person can be directly identified by name, which is the most common identifier. However, a name is not necessary to identify a person, since even other identifiers can be used to “single someone out”. When it is not possible to single out a person from a group, the person can still be considered as identifiable, since combining pieces of information can allow the person to be distinguished.

---

238 Recital 26 of the GDPR. A similar definition can also be found in recital 24 of the DPD.
In addition, the 29WP emphasises that a person who is not yet identified can be considered as identifiable when it is possible to identify this person. According to recital 26 of the DPD, “to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”. The 29WP notes that a mere hypothetical possibility to identify a person is not sufficient. Regard should be given to all factors at stake, such as the cost in conducting identification and the intended purpose. Therefore, if the data is intended to be stored a longer period of time, the possibilities for development in technology should be considered.

As Roosendaal notes, the 29WP gives the notion of ‘personal data’ a broad definition. One of the problematic issues that Roosendaal raises is the cases where the individual is not identifiable today but may be identifiable in the future. This can be the result of for example new data combinations, additional data or technologies that will become available at some point. Hence, it can be difficult to predict whether the data will be identifiable in the future. I agree with Roosendaal that it is problematic to consider data which will be related to an identifiable person in the future, as personal data. In my view, such an interpretation results in uncertainty and unpredictability for both data subjects and controllers.

Recital 26 of the GDPR which clarifies when data is considered as personal data is similar the DPD’s definition of personal data. According to recital 26 of the GDPR, in order to determine whether a natural person is identifiable, “account should be taken of all means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for

---

identification, taking into consideration the available technology at the time of the processing and technological developments.”

The GDPR is much more detailed than the DPD, when it comes to determining whether a natural person is identifiable. This is obviously a welcomed improvement in the GDPR, compared to the DPD. Interestingly, the GDPR does not mention the intended purpose of the processing\textsuperscript{247} as a relevant factor. It is clear from the recital that only objective factors are to be taken into account. Among these factors are technological developments. It can be noted that the problem raised by Roosendaal concerning the impact of potential developments in technology on the applicability of EU data protection law remains when interpreting and applying the GDPR. In other words, in my view the GDPR does not remove the uncertainty when it comes to determining whether certain information will, in the future, be related to an identified or identifiable person. On the other hand, due to the fact that technology develops extremely rapidly, it is not possible to give an exhaustive list of factors that determine whether data, which may at some point identify a person, is to be considered as personal data.

6.4 The broad notion of monitoring

The 29WP is, as noted above, of the view that the notion of monitoring includes all forms of tracking and profiling on the internet\textsuperscript{248} However, the 29WP does not refer to future techniques. It is, in my view, unclear what the 29WP means with its statement that \textit{all} forms of tracking and profiling are included in Article 3(2)(b) of the GDPR. In my opinion, a broad definition of monitoring is especially supported by the argument that it is impossible to predict how the technology will develop in the coming years. Therefore, to restrict the definition to only include some specific forms of tracking would have undesired consequences. The risk would then be that the GDPR would not protect data subjects from online tracking, when new forms of profiling, that do not exist today, are used in the future.

\textsuperscript{247} The 29WP does consider the purpose as a relevant factor under the DPD, see Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p 15-16.

\textsuperscript{248} Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (‘DPOs’), p 8.
At the time when the DPD was drafted, the legislator could not predict all the tracking techniques used in today and how massive the use of new techniques would be. Therefore, it is necessary to take into the consideration that online tracking will surely develop even further in the future.\textsuperscript{249} To only include certain techniques in the scope of application of Article 3(2)(b) of the GDPR and in that way exclude future tracking techniques would not be beneficial for the protection of personal data provided by the Regulation.

On the other hand, including all forms, the existing \textit{and} the future ones, of tracking and profiling can harm legal certainty. If Article 3(2)(b) GDPR covers all possible techniques, controllers or processors, as well as data subjects, cannot know which tracking techniques falls within the territorial scope of application of the GDPR. The notion of ‘monitoring’ becomes unclear which reduces the effectiveness of the Regulation. Also, including the future unknown techniques has an impact on the qualification of data as \textit{personal data}. As noted above, the possibility to identify a person depends on the available technology. New technologies can enable the identification of a person who is not identifiable today but who can become identifiable in a couple of years. That the future techniques fall within the notion of ‘monitoring’ makes it difficult to define ‘personal data’ since it is impossible to know under which circumstances a person can be considered identifiable in the future. It is challenging to regulate something that does not yet exist. Due to the uncertainty regarding the notion of ‘monitoring’ as well as the definition of ‘personal data’, the protection of personal data of data subjects in the EU may not be guaranteed.

As Moerel notes, more or less all websites today use tools such as cookies and JavaScript. She stresses that the expansive interpretation of Article 4(1)(c) of the DPD, supported by the 29WP, to include the use of these tools results in the application of the DPD whenever a controller or a processor processes the data of a person in the EU. Moerel refers to the concept of ‘regulatory overreaching’ which is considered as an unacceptable approach by several commentators.\textsuperscript{250} Bygrave defines the concept of ‘regulatory overreaching’ as “a situation in which rules are expressed as generally and non-discriminatingly that they apply \textit{prima facie} to a large range of activities without having much of a realistic chance

\textsuperscript{250} Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, p 29.
of being enforced.” As an example, Bygrave mentions the websites that set cookies on the browser programs of those who are visiting the particular website. If an Indian website operator uses cookies on its website, and persons present in the EU visit that website, the processing of personal data of those data subjects falls within the scope of EU data protection law. This is the case under the condition that the cookies identify the natural persons visiting the website, so that the criterion of personal data is met.

It can, however, be questioned whether the same can be said about Article 3(2)(b) of the GDPR. In this provision the territorial scope is, compared to Article 4(1)(c) of the DPD, expressed rather clearly. De Hert and Czerniawski are of the view that the clarifications in recital 24 of the GDPR are precise enough. It is clear from Article 3(2)(b) that the GDPR applies to cookies and other tracking techniques. In recital 30 of the GDPR, cookie identifiers are explicitly mentioned as an example of online identifiers that may be used to create profiles of the natural persons and identify them. That the use of cookies is considered as ‘use of equipment’ under Article 4(1)(c) of the DPD is less apparent.

On the other hand, if the GDPR includes all forms of tracking techniques, it could be argued that this is a form of regulatory overreaching since the provision is expressed rather generally. Also, it can be argued that the vague chances of being enforced may not only concern the DPD but also the GDPR.

According to Svantesson, the GDPR “bites off more than it can chew.” Svantesson refers to the broad scope of application of the GDPR. He sees the potential enforcement difficulties as a problem with the Regulation. I too do recognise the potential difficulties to enforce judgments, given in the EU, in third states. Yet, it should not be a reason not to apply EU data protection law in cases where the controller is established in a third country. As already noted, in the internet context the controllers and the processors that process the personal data of data subjects in the EU are often located outside the EU. If

---

251 Bygrave, L, Determining Applicable Law pursuant to European Data Protection Legislation, p 8.
252 Bygrave, L, Determining Applicable Law pursuant to European Data Protection Legislation, p 8.
253 De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.
254 Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, p 232.
255 Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, p 232-233.
the GDPR would only apply to controllers and processors established within the borders of the EU, the legislation would be ineffective. Therefore, in my view the broad territorial scope is justified taken into account the objective of the GDPR to protect data subjects in the EU.

It can also be noted that Article 3(2)(b) of the GDPR does not apply to all websites. Instead, the GDPR does require a connection with the EU. As expressed in Article 3(2)(b), the data subject needs to be present in the EU. In addition, Article 3(2)(b) specifies that the Regulation applies where the processing activities are related to the monitoring of the behaviour of data subjects in the EU “as far as their behaviour takes place within the Union”. Thus, it can be argued that there is a sufficient connection between the processing of personal data and the EU.

6.5 Behaviour that takes place in the EU

Article 3(2)(b) of the GDPR is, as mentioned above, limited to monitoring of behaviour that takes place within the Union. De Hert and Czerniawski are of the view that the requirement “as far as their behaviour takes place within the Union” adds to the provision a tone of moderation and excludes from the territorial scope of the Regulation situations where the connection with the EU is rather weak. De Hert and Czerniawski argue that this limitation excludes the cases where the only connecting factor between the monitoring and the EU is that the data subject is an EU resident. As an example De Hert and Czerniawski give a situation where a European tourist is shopping in New York. In such a situation the connection with the EU is insufficient.256

I agree with De Hert and Czerniawski in that the situation, given as an example, should not be governed by the GDPR. However, I do not agree with De Hert and Czerniaswki regarding their arguments concerning the addition of the criterion “as far as their behaviour takes place within the Union”. Firstly, the GDPR does not require that the data subject is an EU resident. Instead, the GDPR requires that the data subject is present in the EU, regardless of the residence or nationality of the data subject, which was discussed

---

256 De Hert, P, Czerniawski, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.
in Chapter 3. Therefore, this criterion already excludes the situations which have a weak connection with the EU territory, such as the example above. As a result, adding “as far as their behaviour takes place within the Union” to the provision does not, in my view, provide any further clarification or stronger connection with the EU. Besides, is it even possible that a controller monitors the behaviour of a data subject present in the EU, but whose behaviour takes place outside the EU? In my view, the answer to the question is negative.

Furthermore, it can be argued that in an online context, behaviour takes place on the internet and not within the territory of a particular state. On the other hand, it can also be considered that online behaviour takes place in all the states that provide an access to the internet. Consequently, requiring that the behaviour needs to take place within a territory is not compatible with the ‘borderless’ nature of the internet.

Finally, the criterion that the behaviour needs to take place within the EU is in my opinion useless. The fact that the provision requires that the data subject is in the EU also means that the behaviour takes place in the EU. It should not be possible that the data subject is present in the EU while the behaviour of that data subject takes place outside the EU.

6.6 Is an intention to monitor required?

According to De Hert and Czerniawski, Article 3(2)(b) of the GDPR is a good example of the concept of targeting based on a straightforward rationale “you might be targeted by EU law only if you target” (as expressed by de Hert and Czerniawski).²⁵⁷ As discussed in Chapter 5, it is clear that the concept of targeting is used in Article 3(2)(a) of the GDPR. It can, however, be questioned whether the concept of targeting is also used in Article 3(2)(b) of the GDPR.

As already noted, the concept of targeting requires an intention to target. This means that the activity is intended to have effects within a state territory.²⁵⁸ If the concept is used in Article 3(2)(b), the controller needs to target the data subject in the Union, the behaviour

---

²⁵⁷ De Hert, P, Czerniawski, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.
²⁵⁸ Schultz, T, Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface, p 817.
of whom it is monitoring.\textsuperscript{259} More precisely, the controller needs to have an intention to monitor the behaviour of the data subject in question. However, according to recitals 23 and 24, the criterion of ‘envisaging’ only concerns the offering of goods or service in Article 3(2)(a), and not the monitoring of the behaviour in Article 3(2)(b). Instead, Article 3(2)(b) applies when natural persons are tracked on the internet (recital 24). Furthermore, according to recital 23 (concerning Article 3(2)(a)) the mere accessibility of a website is insufficient to ascertain an intention to target. The recital 24 does, on the other hand, not mention anything about the accessibility of a website. The question is whether the notion of tracking includes an intention to monitor or profile data subjects in the EU.

It can be argued that it should not be possible to track or profile someone without any intention to do so. Jay argues that all the three provisions using the notion ‘monitoring’ in the GDPR seems to require “an intentional, on-going, and directed activity”\textsuperscript{260} Jay notes that there is, however, no suggestion that Article 3(2)(b) would require the activity to be directed at achieving any particular end.\textsuperscript{261}

To assume that monitoring includes an intention to target those states where the data subjects are present is in my view problematic. Firstly, it does not appear in the GDPR that Article 3(2)(b) would require an intention to target data subjects in the EU. Secondly, as mentioned above, most of the websites today use cookies or other profiling techniques and are accessible from all those states where the internet is accessible. If the notion of ‘monitoring’ automatically includes an intention to target, then a controller would target all the data subjects that visit the website of the controller. As discussed in Chapter 5, a business may also target the whole world, including all the data subjects using the internet and acting in the online environment. It is, however, unclear whether targeting the whole world is considered as targeting the EU. My interpretation of Article 3(2)(b) of the GDPR is that the provision does not require an intention to target data subjects in the EU. Thus, Article 3(2)(b) should apply regardless of whether the business is targeting data subjects in the EU or not.

\textsuperscript{259} De Hert, P, Czerniawski, M, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, p 238.


Finally, it can be noted that many websites use cookies under the condition that the internet user accepts the use of cookies. By accepting the use of cookies the data subject consents to the profiling and to the processing of her or his personal data. This leads us to the question whether it is possible to agree on the applicable law to the monitoring of the data subject’s behaviour, other than the GDPR. The reasoning in Chapter 5 is also relevant here, and the Facebook example in Chapter 5 can again be used for illustration. According to its website, Facebook uses cookies. When it comes to potential disputes between Facebook and its users, Facebook states that the applicable law is the laws of the state of California.262 As noted in Chapter 5, it should not be possible to escape the protective rules of the GDPR by an agreement on applicable law. The right to the protection of personal data is a fundamental right and the GDPR seeks to protect this fundamental right. Supported by CJEU case law, the GDPR should be interpreted in the light of its objective to protect the processing of personal data of data subjects in the EU.

### 6.7 Cross-border situations that fall outside the territorial scope of the GDPR

Due to its broad territorial scope the GDPR manages to capture the majority of cross-border situations. The GDPR is clearly a step forward compared to the DPD as it is better adapted to the challenges of fast developing technology. Despite its broad applicability, there is a lacunae in the territorial scope of the GDPR. Jay argues that there will be cases where a controller or a processor monitoring the behaviour of data subjects in the EU will fall outside the scope of the GDPR. The same applies when the controller or the processor is offering goods or services to data subjects in the EU.263

Imagine that a controller has two establishments, one in the US and one in the EU. The establishment in the US has a website which uses cookies to monitor the behaviour of the persons visiting the website. There is no connection between the activities of the two establishments. The personal data of the data subjects in the EU is solely processed in the context of the activities of the establishment in the US. Therefore, Article 3(1) is not applicable since the personal data is not processed in the context of the activities of the

---

establishment in the EU. The question is whether Article 3(2) is applicable instead. Article 3(2) applies when the controller or the processor is not established in the EU, but offers goods or services to data subjects in the EU or monitors the behaviour of those data subjects, as far as the behaviour takes place in the EU. In this imaginary case, however, the controller has an establishment also in the EU. As a result, Article 3(2) cannot be applied. This type of cases falls outside the territorial scope of the GDPR which hardly has been the meaning of the EU legislators when drafting the GDPR.\textsuperscript{264}

Moerel notes that the same gap also exists in the territorial scope of the DPD. An extended interpretation of the DPD could result in considering a branch or subsidiary as ‘equipment’, instead of another establishment. This would allow the application of Article 4(1)(c) of the DPD.\textsuperscript{265} This reasoning, although contrary to the wording of the Directive, cannot be used regarding the GDPR since the use of equipment is not a criterion in the GDPR. It was replaced by the two criteria in Article 3(2) of the GDPR, namely offering goods or services to data subjects in the EU and monitoring the behaviour of those data subjects.

As Jay notes, it is however unlikely that EU supervisory authorities would read Article 3 of the GDPR as excluding the situations discussed above. It is also worth taking into account that the CJEU tends to interpret data protection rules in the light of their purpose in order to protect the data subject. It is likely that the CJEU will interpret the territorial scope broadly, covering the hypothetical situation above.\textsuperscript{266}

Hence, it can again be questioned whether such an interpretation is justified. Interpreting Article 3(2) of the GDPR in the light of its objective to protect the processing of personal data of individuals in the EU should not result in an interpretation which is contrary to the wording of the provision. Such an interpretation makes the GDPR unpredictable, and legal certainty is no longer guaranteed. In addition, it has far-reaching consequences both for the data subjects and for the controllers and the processors since the GDPR does not


\textsuperscript{265} Moerel, L, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, 35-36.

clearly determine when it is applicable in cross-border situations. Finally, such an extensive interpretation can hinder the effectiveness of the GDPR.
7 Conclusions

Fast developing technologies are constantly challenging law making, as well as the interpretation and application of legal provisions. As noted in the previous Chapters, data is crossing national borders without difficulty since the internet is not bound by geographical borders. Cross-border data flows comes with possibilities as well as problems. From a private international law perspective, a relevant question that arises regarding these cross-border data flows is the following: What is the applicable law in the cross-border situations where the data subject is in the EU and the controller or the processor is established outside the EU? The GDPR, which will apply from May 2018, strives to provide an answer to this question in its Article 3(2).

This study has analysed and examined Article 3(2) of the GDPR according to which the GDPR is applicable “to 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:\textsuperscript{267}

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.”

Article 3(2) of the GDPR applies to cross-border situations where the data subject is in the EU and the controller or the processor is established outside the EU. The wording in Article 3(2) of the GDPR is new compared to the currently applicable DPD, which requires in its Article 4(1)(c) that when a controller is not established in the EU, the controller makes use of equipment within the EU territory. This study has compared the GDPR with the DPD in order to critically evaluate Article 3(2) of the GDPR and examine whether the territorial scope of the GDPR is an improvement in relation to the DPD.

According to Article 2(2), the GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.\textsuperscript{268} Furthermore, Article 4(1) states that a data subject is an identified or identifiable natural person. The

\textsuperscript{267} Emphasis added.
\textsuperscript{268} Emphasis added.
GDPR applies regardless of the nationality or residence of the data subject (recital 2). Instead, the decisive factor is the physical presence of the data subject within the territory of the EU, as discussed in Chapter 3. As a result, not only EU citizens and residents are covered by the GDPR but also individuals who are temporarily visiting an EU Member State.

Article 3 distinguishes between the situations where the controller or the processor is established in the EU (Article 3(1)) and the situations where the controller or the processor is not established in the EU (Article 3(2)). In order to determine when a controller is not established in the EU, it is essential to determine when a controller is established in the EU. As noted in Chapter 4, the notion of ‘establishment’ is, according to recital 22, “the effective and real exercise of activity through stable arrangements”. In EU case law, the term ‘establishment’ is given a flexible definition and it is to be interpreted in the light of the objective of EU data protection law to protect the processing of personal data of data subjects in the EU. Considering EU case law in the context of data protection law, it can be noted that some physical presence on the EU territory is required in order to be considered as an establishment. Even a person’s physical presence within the EU can be sufficient under the condition that the presence is stable. If the requirements for an ‘establishment’ in the EU are not met, it can be concluded that the controller or the processor is not established within the EU and Article 3(2) may be applicable, instead of Article 3(1) of the GDPR.

However, Article 3(2) does not apply to all cross-border situations where the data subject is physically present in the EU and the controller or the processor is established outside the EU. Article 3(2) further requires that the processing activities are related to the offering of goods or services to data subjects in the EU (Article 3(2)(a)) or to the monitoring of the behaviour of those data subjects (Article 3(2)(b)).

Article 3(2)(a) is explained in recital 23 which states that in order to determine whether Article 3(2)(a) is applicable, it should be ascertained whether it is apparent that the controller or the processor envisions offering services to data subjects in the EU. In addition, the mere accessibility of a website is not sufficient to ascertain such an intention. Recital 23 provides some concrete factors that may make it apparent that a controller envisions offering goods or services to data subjects in the EU. It can be noted that the
The concept of targeting is clearly used in Article 3(2)(a). The targeting approach is new in the context of EU data protection law, but the concept is used in other fields of EU law, such as the consumer law of the EU. Relevant EU case law gives at hand that Article 3(2)(a) seems to be inspired by EU cases where the Court used the concept of targeting, especially the Court’s joint ruling in *Pammer and Hotel Alpenhof*. It is apparent from Article 3(2)(a) that the provision requires an intention to target data subjects in the EU. The GDPR as well as the rulings of the Court where the targeting approach is used seem to focus on a subjective intention. Objective factors, such as the language or currency on a website, can be considered as evidence in order to prove the subjective intention of a business to target data subjects in the EU.

Nevertheless, the problem with the use of the criterion of targeting in data protection context is that it can be difficult to prove an intention to target, for example when none of the objective factors, mentioned in recital 23 and in the cases discussed in Chapter 5, are present. Furthermore, it is unclear whether there is an intention to target data subjects in the EU when a company is acting globally and targeting the whole world. The wording in Article 3(2)(a) requires an intention to specifically target data subjects in the EU, and targeting the entire world without particularly targeting the EU should therefore not fall within the scope of application of Article 3(2)(a). On the other hand, if the GDPR does not apply to these global actors targeting all data subjects, the companies could easily escape the rules of the GDPR by indicating on their websites that they target the whole world. As a result, the protection of the fundamental right to data protection provided by the GDPR would not be effective. As discussed in the previous Chapters, the Court underlines the importance of the purpose of the EU data protection rules and interprets the provisions in the light of the objective of EU data protection law. Consequently, taking into account the objective of the GDPR to protect the processing of personal data of data subjects in the EU, Article 3(2)(a) could be interpreted as covering the situations where businesses target everyone, without specifically targeting the data subjects in the EU. Such an interpretation would, however, be against the wording in Article 3(2)(a). An interpretation against the wording of the provision would result in unpredictability and therefore harm legal certainty.

A data subject may also be in a contractual relationship with a controller. As noted in Chapter 5, a common factor shared by data subjects and consumers is that they are both
considered as a weaker party in relation to a controller or a business. The question is whether the data subject and the controller can choose the applicable law to govern their contract, in accordance with the Rome I Regulation. As discussed in Chapter 5, this should not be possible since it would provide businesses an easy way to avoid the rules of the GDPR. As a result, the GDPR would not effectively protect the data subjects. It can be argued that the GDPR is a *lex specialis* in relation to the Rome I Regulation. The provisions in the GDPR can also be considered as overriding mandatory provisions. The question concerning the GDPR’s relation to the Rome I Regulation is relevant for the application of Article 3(2)(a) as well as Article 3(2)(b) of the GDPR.

The second, alternative, criterion in Article 3(2) is that the controller or the processor, established outside the EU, is monitoring the behaviour of data subjects in the EU as far as their behaviour takes place within the EU. Recital 24 clarifies that in order to apply Article 3(2)(b), it should be ascertained whether data subjects in the EU are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person. The notion of ‘monitoring’ is not defined in the GDPR. However, Article 4(4) of the GDPR provides a definition to the term ‘profiling’ which is to be understood as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

The GDPR is only applicable to situations where processing of *personal data* takes place. The notion of ‘personal data’ is defined in Article 4(1) to mean any information relating to an identified or identifiable person. It has been argued that the notion of ‘personal data’ also covers information related to a person who is not yet identifiable but may become identifiable in the future. Emerging technologies may provide new ways to identify a person and to combine data. However, such a broad definition of ‘personal data’ is problematic since it is difficult to predict what those future techniques will be. For the same reason, it is not possible to give an exhaustive list of factors to determine whether data can, in the future, be considered as personal data.

As noted in Chapter 6, the 29WP is of the view that the notion of ‘monitoring’ includes all forms of tracking and profiling in the online environment, without however referring to future tracking techniques. Here again it can be argued that a general approach to the
The notion of ‘monitoring’ is supported by the fact that it is impossible to predict the future of the fast developing technologies. To restrict the notion to only cover certain forms of tracking would have undesired and unpredictable consequences. As a result, data subjects would not be protected against new forms of tracking that may be used in the future. On the other hand, a broad definition of ‘monitoring’, including both the existing techniques and the future ones, can also harm legal certainty since it is unclear which tracking techniques fall within the definition of ‘monitoring’.

However, Article 3(2)(b) does not apply to all websites since it requires that the data subject is in the EU. In addition, the behaviour of the data subject needs to take place within the EU. Hence, the requirement that the behaviour needs to take place in the EU does not bring any further clarity to the provision or any stronger connection with the EU. When the data subject is physically present in the EU, then the behaviour should also take place in the EU. Therefore, the territorial scope of application of the GDPR would remain the same even if the provision did not expressly require that the behaviour takes place within the EU.

While Article 3(2)(a) requires an intention to target data subjects in the EU, there is no such requirement in Article 3(2)(b). The criterion of ‘envisaging’ appears in recital 23 which clarifies Article 3(2)(a) but not in recital 24 explaining Article 3(2)(b). As noted in Chapter 6, it can be argued that the notion of ‘monitoring’ includes an intention to target data subjects’ behaviour. Such an interpretation is problematic, especially because it does not appear in the GDPR that Article 3(2)(b) would require an intention to target. Article 3(2)(b) of the GDPR should apply regardless of whether the business, which monitors the behaviour of data subjects in the EU, is targeting these data subjects or not.

In general, after having analysed Article 3(2) and compared it to Article 4(1)(c) of the DPD, it can be noted that the GDPR is a step forward because it takes better into account the technological developments. Despite the fact that the broad territorial scope of the GDPR manages to capture the majority of cross-border situations involving a data subject present in the EU and a controller established outside the EU, there are cross-border situations that fall outside the territorial scope of application of the GDPR. This lacunae consists of cases where a third state controller or processor is offering goods or services to data subjects in the EU or monitoring their behaviour, and has an establishment in the...
EU. However, the processing of personal data of the data subject takes place in the context of the establishment in the third state, and therefore Article 3(1) is not applicable. Article 3(2) cannot be applied either since the controller or the processor has an establishment in the EU.

As discussed throughout the study, Article 3(2) of the GDPR includes notions that are rather unclear and provide room for different interpretations. As a result, it is not clear where the boundaries of the territorial scope of the GDPR are. It can, however, be noted that the territorial scope of the GDPR does have boundaries since Article 3(2) of the GDPR requires a connection between the cross-border situation and the EU. The required connection in Article 3(2) is the fact that the data subject is physically present in the EU when the personal data of that data subject is processed by a controller or a processor outside the EU.

New technologies are a challenge for the interpretation and the application of the GDPR. As noted above, there is a risk that Article 3(2) is given a too broad interpretation, in order to take into account the existing as well as the future technologies. A broad interpretation is supported by the objective of the GDPR to protect the fundamental right to data protection of individuals present in the EU. Hence, despite the good intention to protect these data subjects, the GDPR should not be interpreted against the wording in Article 3(2). Such an extensive interpretation would result in unpredictability and harm legal certainty. Consequently, the GDPR would not be effective since it would not be able to provide a sufficient protection to data subjects in the EU. It remains to be seen how the CJEU will interpret Article 3(2) of the GDPR.
Sources

Treaty law and legislation

The European Union

Charter of Fundamental Rights of the European Union (2012/C 326/02), OJ C 326/391

Treaty on European Union (Consolidated Version) of 26 October 2012 (TEU), OJ C 326/13

Treaty on the Functioning of the European Union (Consolidated Version) of 26 October 2012, (TFEU), OJ C 326/47


Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (DPD), OJ L 281/31


Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data
and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1

*International instruments*

United Nations, Universal Declaration of Human Rights, Paris, 10 December 1948


Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981 (Convention 108), ETS 108

*Official documents*

*European Union*

Draft Charter of Fundamental Rights of the European Union – Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4487/00 CONVENT 50, CHARTE 4473/00 CONVENT 49, Brussels, 11 October 2000


European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Version 56 (draft), Brussels, 29 November 2011

Council of Europe

Explanatory Report for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 1981

Hague Conference on Private International Law


Opinions of the Article 29 Data Protection Working Party

Article 29 Data Protection 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, WP 56, adopted on 30 May 2002


Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, WP 179, adopted on 10 December 2010

Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12, WP 225, adopted on 26 November 2014


Case law

*Court of Justice of the European Union*


26/62, *Van Gend en Loos*, delivered on 5 February 1963

Joined cases 28, 29 and 30/62, *Da Costa*, delivered on 27 March 1963

6/64, *Costa v. E.N.E.L.*, delivered on 15 July 1964


C-381/98, *Ingmar*, delivered on 9 November 2000

C-101/01, *Bodil Lindqvist*, delivered on 6 November 2003

Joined cases C-585/08 and C-144/09, *Pammer and Hotel Alpenhof*, delivered on 7 December 2010

C-324/09, *L’Oréal and Others*, delivered on 12 July 2011

C-190/11, *Mühlleitner*, delivered on 6 September 2012

C-173/11, *Football Dataco and Others*, delivered on 18 October 2012

C-218/12, *Emrek*, delivered on 17 October 2013

C-131/12, *Google Spain and Google*, delivered on 13 May 2014


*Opinions of Advocate Generals*

Opinion of Advocate General Trstenjak, joined cases C-585/08 and C-144/09, *Pammer and Hotel Alpenhof*, delivered on 18 May 2010

Opinion of Advocate General Jääskinen, C-324/09, *L’Oréal and Others*, delivered on 9 December 2010
Opinion of Advocate General Jääskinen, C-131/12, Google Spain and Google, delivered on 25 June 2013

Opinion of Advocate General Cruz Villalón, case C-230/14, Weltimmo, delivered on 25 June 2015

Literature


Bogdan, M, Ordre public, internationellt tvingande rättsregler och kringgåendeläran i EG-domstolens praxis rörande internationell privaträtt, SvJT 2001, p 329-346


Brkan, M, Data Protection and European Private International Law, EUI Working Paper RSCAS 2015/40, Robert Schuman Centre for Advanced Studies, Florence School of Regulation, Italy 2015


Kokott, J, Sobotta, C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law (Oxford University Press), Volume 3, Number 4, 2013, p 222-228


Kuner, C, Extraterritoriality and regulation of international data transfers in EU data protection law, International Data Privacy Law (Oxford University Press), Volume 5, Number 4, 2015, p 235-245

Kuner, C, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013


Lipton, J, Rethinking Cyberlaw: A New Vision for Internet Law, Edward Elgar Publishing, UK 2015

Lutzi, T, Internet Cases in EU Private International Law: Developing a Coherent Approach, accepted for publication in the International & Comparative Law Quarterly on 26 April 2017, available at: https://ora.ox.ac.uk


Reding, V, Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world, Speech of the Vice-President of the European Commission,


Schultz, T, Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface, The European Journal of International Law, Volume 19, Number 4, 2008, p 799-839


Stone, P, Territorial targeting in EU private law, Information & Communications Technology Law, Volume 22, Number 1, 2013, p 14-26

Svantesson, D, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, International Data Privacy Law (Oxford University Press), Volume 5, Number 4, 2015, p 226-234

Additional internet sources

Official Website of Facebook, https://www.facebook.com/

Official Website of Snap Inc. (Snapchat), https://www.snapchat.com/l/en-gb/