The concept of ‘transfer’ of data under European data protection law

In the context of transborder data flows

Candidate number: 8026
Submission deadline: 01.12.2015
Number of words: 17 454
# Table of contents

ACKNOWLEDGEMENTS ......................................................................................................................... IV

1 INTRODUCTION ........................................................................................................................................ 1

1.1 Background ........................................................................................................................................... 1

1.2 Matter at hand ....................................................................................................................................... 5

1.3 Methodology and structure of the thesis .............................................................................................. 8

2 GENERAL OVERVIEW OF THE EU REGIME ON TRANSFER OF PERSONAL DATA OUTSIDE THE EEA .......................................................................................................................... 11

2.1 Introduction .......................................................................................................................................... 11

2.2 The principles ...................................................................................................................................... 11

2.3 The derogations ................................................................................................................................... 13

2.3.1 Exceptions under Article 26(1) ........................................................................................................ 13

2.3.2 Adduced adequate safeguards under Article 26(2) ......................................................................... 14

2.3.3 Summary ......................................................................................................................................... 16

2.3.4 Proposed changes ............................................................................................................................ 16

3 CJEU CASE LAW: C-101/01 *(LINDQVIST)* ............................................................................................. 19

3.1 Introduction .......................................................................................................................................... 19

3.2 Facts and findings ................................................................................................................................ 19

3.3 The Court’s justification ...................................................................................................................... 21

3.3.1 The first justification ....................................................................................................................... 21

3.3.2 The second justification .................................................................................................................. 22
3.3.3 The third justification ................................................................. 23

3.4 Implications .................................................................................. 24
  3.4.1 Introduction ............................................................................. 24
  3.4.2 Technical factors ................................................................. 25
  3.4.3 Consequences ....................................................................... 26

4 NATIONAL LAW ................................................................................ 32
  4.1 Introduction ................................................................................ 32
  4.2 Norway ..................................................................................... 33
    4.2.1 The Norwegian PDA ........................................................ 33
    4.2.2 The Norwegian DPA and the Norwegian Privacy Appeals Board .... 35
    4.2.3 Commentaries by scholars .................................................. 36
  4.3 Germany ..................................................................................... 37
  4.4 United Kingdom ........................................................................ 37
  4.5 Australia ..................................................................................... 38
    4.5.1 Introduction and issues assessed ........................................ 38
    4.5.2 Assessment .......................................................................... 39
    4.5.3 ALRC’s conclusion ............................................................. 41
  4.6 Summary and consideration ..................................................... 42

5 DE LEGE FERENDA ......................................................................... 44
  5.1 Introduction ................................................................................ 44
  5.2 Disadvantages of defining the concept ’transfer’ of data .............. 44
  5.3 Advantages of defining the concept ’transfer’ of data .................. 46
  5.4 Should ’mere transit’ be distinguished from ’transfer’ of data? ...... 49
5.5 Summary ...................................................................................................................... 51

6 CONCLUSION ................................................................................................................. 51

7 TABLE OF REFERENCE ................................................................................................. 56

Books and journal articles ............................................................................................... 56

Reports, opinions and other documents ........................................................................ 57

Legislation ......................................................................................................................... 60

Case law of the Court of Justice of the European Union ................................................ 61

Decisions by the Norwegian Privacy Appeals Board ...................................................... 62
**Acknowledgements**

I would like to express my greatest gratitude to Asgeir Giskegjerde for priceless support during the writing of this thesis, as well as my family and friends who have been beyond supportive. I also want to thank my supervisor, Line Marianne Coll, for outstanding supervision, support and inspiration.
1 Introduction

1.1 Background

With the global economy gone digital and the Internet facilitating increased communication across borders, there is no doubt that information technology plays a more crucial role than ever before. Companies in almost every sector of modern economy depend on innovations driven by personal data to do business. In this context, personal data plays an increasingly important role. Consequently, both processing of personal data and the amount of personal data that is processed has increased significantly.\(^1\) Personal data has become goods to trade, and has even been described as ‘the new oil’.\(^2\) In this picture, the international transfer of personal data has had a positive impact on global business, while at the same time subjecting the privacy of individuals to new and increased risks.\(^3\)

In Europe, the body of law that is aimed at regulating the processing of data on individual natural persons (data subjects)\(^4\) tends to be described as ‘data protection law’. The primary objective of this body of law is to safeguard the privacy-related interests of those persons when data about them is processed. In New Zealand, North America and Australia the term ‘privacy law’ tends to be used.\(^5\) For the purpose of this thesis, the term ‘data protection’ will be used, as the main focus is on European data protection legislation.

While the terms ‘data protection’ and ‘privacy’ are closely linked, it has been stressed in Europe that the terms are not identical. The protection of privacy is a widely recognised


\(3\) Kuner, *Transborder Data Flows and Data Privacy Law*, 1.

\(4\) Hereinafter, individual natural persons will be referred to either as ‘data subjects’ or as ‘individuals’.

\(5\) Bygrave, *Data Privacy Law*, xxv.
human right⁶ that includes the right to be let alone from intrusion from others⁷, while data protection refers to principles on the processing of data which is directly or indirectly related to identified or identifiable individuals. On the one hand, ‘data protection’ is narrower than privacy, as the right to privacy encompasses more than principles regarding processing of personal data. On the other hand the term encompasses a wider area, since ‘data protection’ serves a broader range of interests⁸ than simply privacy.⁹

In Europe, the processing of personal data about individuals is regulated by the Data Protection Directive 95/46/EC¹⁰ (hereinafter ‘DPD’ or ‘the Directive’), which is legally binding in the 28 EU member states and the three EEA member countries.¹¹ The primary goals of the Directive are twofold and explicitly stated in recitals to the Directive¹² and in Article 1.¹³ The first aim relates to the concern of promoting the realization of the internal market of the EU, whereas goods, persons, services, capital and, concomitantly, personal

---

⁶ See primarily Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the subsequent provisions within the framework of the European Union.

⁷ Bygrave, Data Privacy Law, 24.

⁸ Such as the right not to be discriminated, see European Data Protection Supervisor (EDPS), “Public access to documents and data protection,” 15. The EDPS is tasked with ensuring that EU institutions and bodies respect people’s right to privacy when processing their personal data. Among other things it advises EU legislators on data protection issues in various policy areas and new legislative proposals, see European Union, “European Data Protection Supervisor (EDPS).”

⁹ Bygrave, Data Privacy Law, 26 and EDPS, “Public access to documents and data Protection,” 15.

¹⁰ Officially ‘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’.

¹¹ See Decision of the EEA Joint Committee No. 83/1999 of June 1999 amending Protocol 37 and Annex XI (telecommunication services) to the EEA Agreement. The EEA member countries are Iceland, Liechtenstein and Norway.

¹² See especially recitals 2, 3, 5, 7, 10 and 11.

¹³ Implemented in the Norwegian Personal Data Act 2000 (hereinafter ‘PDA’) section 1.
While the Directive strives to ensure a high level of data protection across the EU, it is unique in the sense that it prohibits the restrictions of flow of personal data between the EU and EEA member states on the grounds of privacy and other basic human rights, cf. Article 1(2) of the Directive. At the same time, Chapter IV of the Directive that regulates transfer of personal data to so-called ‘third countries’ (that is, countries outside EU and EEA), prohibits by its Article 25(1) the transfer of personal data to countries that do not provide an adequate level of protection, in the cases that the exceptions in Article 26(1) are not applicable and in the absence of adduced adequate safeguards under Article 26(2) of the Directive. In light of the extreme value of personal data in today’s information society, prohibition of transfer of personal data to a country can have a significantly negative economic impact.

However, determining whether or not ‘transfer’ of data, within the meaning of Chapter IV of the Directive, has taken place is not always an easy task, as the concept ‘transfer of personal data’ is not defined in the Directive. In the 1970s, the term ‘transfer’ of data was

---

14 Bygrave, *Data Privacy law*, 57 and DPD Article 1 and recitals 2, 3, 5, 7, 10 and 11.
15 Bygrave, *Data Privacy law*, 57.
16 Implemented in PDA Chapter V.
17 See also recital 57 of the Directive. Article 25(1) is implemented in PDA section 29(1).
18 Whilst acknowledging in recital 56 of the Directive that transfers of personal data from a member state to third countries are necessary for the expansion of international trade.
19 Implemented in PDA section 30(1).
20 Implemented in PDA section 30(2).
21 Elaborated upon in detail in chapter 2.4.2.
22 Hereinafter referred to as ‘transfer’ of data or ‘transfer’.
typically understood to refer to point-to-point transmissions. The nature of transfers has by contrast now changed so they no longer constitute point-to-point transmissions, but “occur as a part of networked series of processes made to deliver a business result.” Moreover, the difficulties associated with determining whether ‘transfer’ of data has taken place are increased by the fact that the Internet itself is structured to transit data and is not based on geography, but rather on technical parameters. The Internet does thus not recognise geographical borders in the absence of specific technology. Data protection and privacy is on the contrary dependent on information being kept within geographical borders. Due to this fact, it is not only difficult to determine where the data itself is located, but also what rules regulate its processing. As a consequence of the borderless Internet, it is therefore hard to determine when and how data is actually transferred over geographical borders, as no such borders exist on the Internet.

Before introducing the topic that will be the main subject matter of this thesis, it is worth noting that the Directive does provide some useful definitions and clarifies the Directive’s scope in Articles 2 and 3, even though it does not define what constitutes ‘transfer’ of data. Regarding its scope, it extends to most stages in the processing of personal data, which is data that relates to and allows identification of an individual, cf. DPD Article 2(a). The notion of ‘personal data’ should be interpreted widely. ‘Processing of personal data’ refers *inter alia* to the way the personal data is disclosed by transmission, disseminated or otherwise made available, cf. DPD Article 2(b). This includes ‘transfer’ of data,

26 Svantesson, “Privacy, Internet and Transborder Data Flows,” 1.
27 Implemented in PDA sections 2 and 3.
28 See Article 3 of the Directive.
29 Implemented in PDA section 2(1).
31 Implemented in PDA section 2(2).
meaning that ‘transfer’ of data is seen as constituting a form of processing in the terms of the Directive.\textsuperscript{32}

The entities that bear the main obligation for complying with the data protection legislation are the natural and legal persons that determine the purposes and means of the processing of the personal data, referred to as ‘controllers’ under Article 2(d) of the Directive.\textsuperscript{33} They are also responsible for ensuring that ‘processors’\textsuperscript{34} that process personal data on their behalf, comply with applicable data protection requirements.\textsuperscript{35}

For multinational companies established both within the EU/EEA and outside, it can be very complex and cumbersome to ensure compliance with all applicable data protection requirements. For example, some data protection laws require controllers to register transfers of data with a regulatory authority before they are carried out, which may involve considerable effort.\textsuperscript{36} Another aspect of this complexity is that controllers established within the EU/EEA must comply with Chapter IV of the Directive, including the requirement provided for in Article 25(1), that they are prohibited from transferring personal data to a country that does not ensure an adequate level of protection, in the absence of adduced ‘adequate safeguards’. This means that the Directive sets limits to intra-group transborder transfers of data, as well as on daily transborder transfers of data in business operations.

\subsection{1.2 Matter at hand}

The DPD does not define what constitutes ’transfer’ of data. Determining what constitutes ‘transfer’ is however of importance in practice, as if no ’transfer’ of data takes place, then

\begin{flushleft}
\textsuperscript{32} Kuner, \textit{European Data Protection Law}, 79.
\textsuperscript{33} Implemented in PDA section 2(4).
\textsuperscript{34} Defined in DPD Article 2(e).
\textsuperscript{35} Bygrave, \textit{Data Privacy Law}, 17.
\textsuperscript{36} Kuner, \textit{Transborder Data Flows and Data Privacy Law}, 17.
\end{flushleft}
the processing operation in question does not come under the scope of Chapter IV of the DPD. In such cases there is no need to assess whether a third country ensures an adequate level of protection or not, nor is it necessary to take measures in order to provide additional safeguards for the data in question. This can be very important for multinational companies and companies that use outsourcing and cloud computing in their activities, as the costs of and difficulties in complying with these requirements may be substantial. The subject of this thesis is therefore if and then possibly how, one should define the concept of 'transfer' of data in European data protection law.

Even though the concept 'transfer' of data is not defined in the DPD, some international regulatory instruments provide a definition of the concept of 'transborder flows of personal data', which is equivalent to the concept of 'transfer' of data.37 Those instruments are the OECD Privacy Guidelines and Council of Europe Convention 108, which are both of relevance for many EU/EEA member states. In the OECD Privacy Guidelines, 'transborder flows of personal data' are defined as "movements of personal data across national borders", cf. § 1(c). The Council of Europe Convention 108 defines 'transborder flows of personal data' as the "transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed", cf. Article 12(1). Even though these definitions may provide a certain guidance as to what constitutes 'transfer', they leave other and more problematic issues untouched; namely when and how personal data crosses national borders, especially in the context of the Internet. One of the issues I will assess is thus whether selected national laws provide a further useful guidance on the issue.

One issue related to when and how personal data crosses national borders in the context of the Internet is whether and how one should distinguish between 'mere transit' and 'transfer' of data. As a point of departure, the fact that personal data is transferred via the Internet

37 Kuner, Transborder Data Flows and Data Privacy Law, 11.
from one EU/EEA member state to another, meaning that it may be routed across the borders of a non-EU/EEA country due to the architecture of the Internet, does not constitute 'transfer' of data. This applies as long as the presence of the data in a non-EU/EEA country is limited to 'mere transit' and no further processing is performed on it there.\(^\text{38}\) However, the distinction between 'mere transit' and 'transfer' of data is uncertain to some extent, as the Directive does not define these concepts.\(^\text{39}\) This is one of the issues that will be assessed in the thesis, as it is materially linked to the definition of 'transfer' of data.

When looking into what constitutes 'transfer' of data, the main argument in this thesis is that an intention to make data accessible to parties in third countries, and the purpose of the transaction are factors that play an important role when determining whether or not 'transfer' of data takes place. Further, the risks associated with the 'transfer' play an important role when determining whether restrictions on 'transfers' come into play or not.

In addition to the requirements in Chapter IV of the DPD, 'transfer' of data is also seen under the national laws of most EU member states, as constituting a form of processing in the terms of the Directive.\(^\text{40}\) This means that not only do controllers have to comply with the requirements of Chapter IV when transferring data, but also with the basic requirement set out in Article 7 (and Article 8 when sensitive personal data is processed), that there is a legal basis for the transfer.\(^\text{41}\) In other words, if someone other than the controller gains access to personal data through the transfer, it must be ensured that the data subject consented

\(^{38}\) However, such a transfer would constitute an intra-EU 'transfer' for data protection purposes, see Kuner, *European Data Protection Law*, 156.

\(^{39}\) Kuner, *Transborder Data Flows and Data Privacy Law*, 16.

\(^{40}\) Kuner, *European Data Protection Law*, 79.

\(^{41}\) Implemented in PDA sections 8 and 9.
to the transfer or the transfer is covered by a processing exception provided for in Article 7 or Article 8 of the Directive.\textsuperscript{42} Deciding whether personal data may be transferred outside the EU/EEA is thus a two-step process, as the personal data must first be legally collected and processed under the Directive, and then there must be a legal basis for the transfer outside the EU/EEA under Chapter IV of the Directive\textsuperscript{43} to ensure that they data will enjoy ’adequate protection’ in the third country in question.\textsuperscript{44}

’Transfer’ of data as a form of processing will not be included in the scope of this thesis. Further, this thesis will not discuss issues regarding exemptions from the Directive’s scope. Note that Article 3(2) of the Directive exempts the processing of data ’by a natural person in the course of a purely personal or household activity’. Such activities are not included in the scope of this thesis, even though they may raise certain issues of special relevance to ’transfer’ of data. It must also be noted that this thesis will not focus on ’transfer’ of data other than personal data, as defined in Article 2(a) of the Directive. Further, issues relating to ’onward transfer’, meaning further transfers of data from the country of import\textsuperscript{45}, are not included in the scope of this paper.

\subsection*{1.3 Methodology and structure of the thesis}

I will start by providing a general overview of the EU regime on transfer of personal data outside the EU/EEA in chapter two. As the focus of this thesis is on European data protection law, the DPD will be at the heart of this thesis. The meaning and the scope of relevant provisions of the DPD will be analysed in order to assess whether they provide a clarification as to the meaning of the concept of ’transfer’ of data. Opinions from the Article 29

\textsuperscript{42} Or in practice, their implementation in national law. See Hoeren et. al., \textit{Legal Aspects of Digital Preservation}, 76.

\textsuperscript{43} Chapter IV consists of Articles 25 and 26, implemented in PDA Chapter V; sections 29 and 30.

\textsuperscript{44} Kuner, \textit{European Data Protection Law}, 160.

\textsuperscript{45} Kuner, \textit{Transborder Data Flows and Data Privacy Law}, 44.
Data Protection Working Party (hereinafter ’A29WP’), that is established under Article 29 of the Directive, will also be taken into account where relevant, as its opinions have a considerable persuasive authority, even though it is not authoritative. Furthermore, CJEU’s recent decision in C-362/14 (Schrems) will be taken into account to the extent applicable for the purposes of chapter two.

The Court of Justice of the European Union (hereinafter ’CJEU’) has only handed down one decision, C-101/01 (Lindqvist), directly related to the issue. Being the only decision from this authority, the decision deserves due attention and will be analysed in depth in chapter three, to the extent it casts a light on what constitutes ’transfer’ of data within EU law.

In chapter four, I will look at certain national laws and their approaches to define the concept of ’transfer’ of data, and whether they differentiate between ’transfer’ and ’mere transit’. I will start by looking at Norway and assess how Chapter IV of the DPD has been implemented in Chapter V of the Norwegian PDA. Chapter V of the PDA will be assessed and criticised where appropriate. Further, a look will be taken at relevant decisions from the Norwegian Privacy Appeals Board (Personvernemnda), statements from the Norwegian data protection authority (Datatilsynet) and commentaries by scholars. Following that, some attention will be given approaches regarding the concept taken in Germany, the United Kingdom and in Australia. Approaches by data protection authorities and commentaries by scholars will also be taken into account. What implications these

\[\text{\footnotesize{46} Articles 29 and 30 of the PDA.}\]
\[\text{\footnotesize{47} Data protection authorities (DPAs) are national, public independent authorities that are responsible for monitoring and enforcing the application within their territory of the provisions adopted by member states pursuant to the Directive, cf. Article 28(1) of the Directive. They are entrusted several functions, inter alia, the function of examining, with complete independence, whether the transfer of data to a third country complies with the requirements laid down by the Directive, cf. Article 28 and C-362/14 (Schrems), paragraph 57.}\]
various approaches have for the purposes of this thesis will be analysed in the end of chapter four. Chapters two to four address how the concept of ‘transfer’ of data under current data protection laws and in the light of case law and various approaches by scholars and data protection authorities is to be defined, by discussing de lege lata.

In chapter five, I will address the need for a change and improvement in a possible new legal framework under the proposed General Data Protection Regulation\(^48\) (hereinafter GDPR) by discussing whether one should define ‘transfer’ of data by discussing de lege ferenda.\(^49\) I will further discuss whether and how one should differentiate the concepts of ‘transfer’ of data and ‘mere transit’. Throughout the thesis, reference will be made to proposed amendments in the GDPR where appropriate.

Finally, in chapter six, I will suggest how the concept could be defined and discuss factors that should be decisive when defining the concept. Arguments will be put forward to support the conclusion, in light of a holistic analysis of all the aforementioned factors.

\(^{48}\) European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to processing of personal data and on the free movement of such data (General Data protection Regulation).”

\(^{49}\) It may be noted that as of today, the GDPR fails to define ‘transfer’ of data as is the case with the current DPD.
2 General overview of the EU regime on transfer of personal data outside the EEA

2.1 Introduction

In this chapter I will provide a general overview of the EU regime on transfer of personal data outside the EEA, by discussing the provisions of Chapter IV of the DPD that regulate transfer of personal data to third countries.

First I will carry out an analysis of Article 25 of the Directive that sets out the principles that govern such transfers, and then I will discuss the derogations from those principles, as described in Article 26 of the Directive.

2.2 The principles

As previously noted, the point of departure is that the free flow of personal data between EU/EEA member states cannot be restricted for reasons connected with the 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, cf. Article 1(2) of the Directive. This prohibition is based upon the assumption that implementation of the Directive results in equivalent levels of data protection across the EU/EEA, as expressed in recitals 8 and 9 of the Directive.50

The same does not apply to third countries outside the EU/EEA, as Article 25(1) of the Directive prohibits transfers of personal data to a third country if the third country in question does not ensure an adequate level of protection.51 This prohibition applies, according to the wording of Article 25(1), to transfers of "personal data which are undergoing processing or are intended for processing after transfer." In other words, transfer of

50 Bygrave, Data Privacy Law, 191.
51 See also recital 57 of the Directive.
personal data to countries outside the EU/EEA may only take place if the third country in question ensures an adequate level of protection.

The reference to "which are undergoing processing or are intended for processing after transfer" is quite important, as it sets out the prerequisite for the applicability of the provision. This may be exemplified by CJEU’s decision in C-362/14 (Schrems), where the act of Facebook Ireland of transferring personal data of users to servers belonging to Facebook Inc. located in the United States, for the purposes of undergoing processing, was deemed to constitute 'transfer' of data within the meaning of the Directive.\(^{52}\)

How adequacy of the level of protection afforded by a third country is to be assessed is set out in Article 25(2)\(^{53}\) of the Directive. According to Article 25(2), the adequacy shall be assessed in light of all the circumstances surrounding a data transfer operation or set of such operations.\(^{54}\) This assessment lies often firstly with the data exporters and with national DPAs, but the European Commission has on the other hand the power to determine, on the basis of Article 25(6), whether a third country ensures an adequate level of protection by reason of its domestic law or the international commitments it has entered into. The effect of such a decision is that personal data can flow from all the EU/EEA countries to that third country, without any further safeguards being required.\(^{55}\) At the same time, if the Commission finds that a third country does not ensure an adequate level of protection, member states shall take the measures necessary to prevent any transfer of data of the same type to the third country in question, cf. Article 25(4) of the Directive.

\(^{52}\) C-362/14 (Schrems), paragraph 27.

\(^{53}\) Implemented in PDA section 29(2).

\(^{54}\) The factors that shall be given particular consideration in the adequacy assessment are the nature of the data, the purpose and duration of the proposed processing operation(s), the country of origin and country of final destination, the rules of law in force in the third country in question and the professional rules and security measures which are complied with in that country.

\(^{55}\) European Commission, “Commission decisions on the adequacy of the protection of personal data in third countries.”
The countries that are recognised by the European Commission as providing an adequate level of protection by an adequacy decision are often referred to as pre-approved countries. So far, the European Commission has recognized several countries\(^\text{56}\) as providing adequate protection, as well as the United States under the Safe Harbour agreement.\(^\text{57}\) However, it must be emphasized that the CJEU has the power to invalidate the European Commission’s adequacy decisions, and has done so in its recent decision in C-362/14 (Schrems), which was handed down October 6th 2015. By its decision, the Court more specifically declared the Commission’s decision on the EU-US Safe Harbour invalid, which means that it can no longer be relied on as the basis for transfer of data from the EU/EEA countries to the US.

### 2.3 The derogations

#### 2.3.1 Exceptions under Article 26(1)

Despite the requirement of adequacy in Article 25, its impact is mitigated to a significant extent due to the derogations that are set out in Article 26 of the Directive. The derogations in Article 26 of the DPD permit transfer of personal data to a third country even though it lacks an adequate level protection, if the proposed transfer takes place under certain conditions.\(^\text{58}\) Those conditions may be divided firstly to exceptions as set out in Article 26(1), and secondly to adduced adequate safeguards as set out in Article 26(2).\(^\text{59}\) This means in other words, that transfer of personal data for all the countries that are not member states of the EU/EEA or are pre-approved by the Commission, is only allowed by relying on one of the derogations in Article 26.

---

\(^\text{56}\) At the time of writing, these countries are Andorra, Argentina, Canada (for commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

\(^\text{57}\) European Commission, “Commission decisions on the adequacy of the protection of personal data in third countries.”

\(^\text{58}\) Bygrave, Data Privacy Law, 193.

\(^\text{59}\) Esayas, “A walk in to the cloud and cloudy it remains,” 664.
The exceptions in Article 26(1) that may be relied on under Article 26(1) in order to transfer personal data lawfully to countries that do not provide adequate protection, may be divided into six various alternatives. The first exception is if the data subject has given his unambiguous consent to the proposed transfer. The other five exceptions encompass situations where transfer is necessary for certain reasons, such as for performing a contract between the data subject and the controller or a contract concluded in the data subject’s interest between the controller and a third party, or for protecting the vital interests of the data subject.\textsuperscript{60}

Even though these exceptions may be useful in certain cases, it is important to note that they are subject to various restrictions and limitations, which are especially relevant with regard to the use of the consent exception. The A29WP has for example indicated that it is unlikely that consent can provide an adequate long-term framework for controllers in cases when transfers repeatedly or structurally take place for the processing in question, as the consent must, in order to be valid, be a clear and unambiguous indication of wishes, freely given, specific and informed.\textsuperscript{61}

\subsection*{2.3.2 Adduced adequate safeguards under Article 26(2)}

A further derogation is permitted by Article 26(2) if the controller adduces adequate safeguards for protecting the privacy and fundamental rights and freedoms of the data subject. It is further expressly stated in the provision that such adequate safeguards may in particular result from appropriate contractual clauses. The provision foresees the use of binding contractual commitments between the entity that exports the data and the entity

\textsuperscript{60} See Article 26(1) of the Directive for further exceptions.

that imports the data, and obligates both entities to provide certain enumerated protections for the data processing.  

Two kinds of clauses may be used. The first one are so-called ’standard contractual clauses’ that the European Commission has the power to pre-approve as is the case under Article 25, cf. Article 26(4), and are supposed to be used without change.  

The European Commission has exercised its power by issuing standard contractual clauses that may be used in order to govern transfer(s) of data.  

The second kind are so-called ’ad hoc’ clauses, that are custom-drafted in each case by the parties and requires often the approval of the local DPAs.  

Another form of adequate safeguards in the meaning of Article 26(2), although it is not explicitly mentioned in the Directive, are Binding Corporate rules (hereinafter ’BCRs’). BCRs are internal, legally binding data processing rules adopted by a multinational group of companies, which are enforceable against each entity in the corporate group, regardless of their location. BCRs grant certain rights to the data subjects and define the company’s global policy regarding international transfers of personal data within the same corporate group. BCRs are an alternative from the use of standard contractual clauses, and may be preferable when it becomes too burdensome for companies to sign contractual clauses for each transfer made within a corporate group.

62 Kuner, Transborder Data Flows and Data Privacy Law, 43.  
63 Kuner, Transborder Data Flows and Data Privacy Law, 43.  
Unlike the standard contractual clauses, the European Commission does not have the power to issue adequacy decisions on BCRs, as BCRs are not mentioned in the Directive. BCRs are thus approved by the national DPAs instead. Most, but not all DPAs, recognise the possibility for companies in the EU/EEA to use BCRs as a legal basis to export personal data, if they are recognised as providing 'adequate safeguards’ under Article 26(2). The conditions for approval of BCRs differentiate however between various EU/EEA member states. The DPAs have though created a procedure that is designed to lead to a mutual recognition of approvals of BCRs, even though not all DPAs recognize it yet. Once BCRs have been approved by appropriate DPAs, they allow for transborder transfers of data within the entire corporate group, as the personal data receives the same protection wherever it goes within the corporation.

2.3.3 Summary

In summary, the Directive allows for transfer of data to third countries that do not provide adequate protection, on three possible legal bases: The first one being an adequacy decision from the European Commission. The second legal basis is provided for under one of the derogations in Article 26(1), and the third alternative is to adduce 'adequate safeguards’ under Article 26(2) in the form of standard contractual clauses, ’ad hoc’ clauses or BCRs.

2.3.4 Proposed changes

In January 2012, the European Commission officially adopted a proposal for a General Data Protection Regulation (GDPR) that will, if enacted, replace the DPD. The proposal is however still subject to EU legislative procedures at the time of writing, and might thus

---

66 Kuner, Transborder Data Flows and Data Privacy Law, 44.
67 European Commission, “What is mutual recognition?”
68 Kuner, Transborder Data Flows and Data Privacy Law, 43-44.
still be subject to change. As the GDPR would make a number of major changes to the existing EU regime on transfer of data, it is worth noting some of the main changes in the proposal.

Firstly, the presumption under the DPD that personal data may not be transferred unless the third country provides ‘adequate level of protection’ is abandoned by Article 40 of the GDPR, that requires instead compliance with all provisions of the Regulation, including the ones on international transfer.69 The GDPR maintains the three legal basis for international transfers of data70, but does make a few changes to the existing legal bases under the DPD.

One major change is that the GDPR expands the scope of Commission adequacy decisions by providing that they may cover not only an entire country, but also a territory within a third country, an international organization or a processing sector, cf. Articles 41(1) and 41(3). This may lead to increase of adequacy decisions, which have not been many under the current Directive. The assessment of adequacy does however differentiate significantly from the current approach, as restrictions are still, as a point of departure, to be imposed by using an adequacy test.71

Another change is that the GDPR specifically provides for the use of BCRs as appropriate safeguards in Article 43, including the use of BCRs for processors. The use of BCRs will be limited to companies in the same corporate group of undertakings, cf. recital 85 in the GDPR, and follow the requirements contained in Article 43.

Further, the use of derogations to transfer data is allowed under GDPR Article 44, but their scope differentiates in some aspects from Article 26 of the Directive. Particularly, new

69 Kuner, Transborder Data Flows and Data Privacy Law, 46-47.
70 See Article 41 (Commission adequacy decisions), Article 42 (appropriate safeguards) and Article 44 (derogations) of the GDPR.
71 Bygrave, Data Privacy Law, 198 and Kuner, Transborder Data Flows and Data Privacy Law, 47.
restrictions on the use of consent are introduced in Article 44(1)(a). This is due to the fact that growing concerns exist regarding that individuals may not realize what they are consenting to, and therefore may not have a meaningful opportunity to refuse to consent.\textsuperscript{72}

Another significant change is found in GDPR Article 44(1)(h), which provides that transfer of data may in limited circumstances be justified on the basis of the legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of that transfer operation, and not for transfers that can are frequent or massive.\textsuperscript{73} Otherwise, the derogations under Article 44 GDPR are quite similar to the derogations provided for in Article 26(1) of the Directive.\textsuperscript{74}

What may be said is that under both the regime on transfer of personal data in the current Directive and in the GDPR, transfer of personal data to third countries outside the EU/EEA is subject to various requirements and restrictions. This fact underlines the importance of defining what constitutes ’transfer’ of data within EU law, as it is determinative for whether or not these rules come into play.

This chapter has discussed the rules that must be complied with in order to transfer data to a third country outside the EU/EEA and has illustrated the importance of defining what constitutes ’transfer’ of data. In the next chapters I will thus carry out an analysis of the concept ’transfer’ of data, starting by discussing case law from the CJEU on the topic in chapter three.

\textsuperscript{72} Kuner, \textit{Transborder Data Flows and Data Privacy Law}, 47.

\textsuperscript{73} See Article 44 GDPR and European Commission, “Explanatory Memorandum” (to the GDPR), 12.

\textsuperscript{74} Bygrave, \textit{Data Privacy Law}, 198.
3 CJEU case law: C-101/01 (*Lindqvist*)

3.1 Introduction

The case law of the CJEU is undisputedly one of the most important sources in EU law and is the ultimate arbiter of EU law, including data protection law. The Court has rendered several decisions interpreting the DPD, but only one decision, C-101/01 (*Lindqvist*), that can be found to be of relevance to the definition of the concept of ‘transfer’ of data. Accordingly, the decision deserves an analysis.

I will start by describing the facts of the case and the findings of the court. Then I will continue on discussing the court’s justification for its conclusion, and point out aspects that have been subject to criticism by scholars. Following that I will discuss the implications of the decision and the extent it provides a useful guidance for defining what constitutes ‘transfer’ of data.

3.2 Facts and findings

In *Lindqvist*, a Swedish woman, Mrs Lindqvist, who worked as a catechist in the parish of Alsedå in Sweden, had set up internet pages at home on her personal computer, following a data processing course that she had taken. On the internet pages she made available information about herself and 18 of her colleagues in the parish, sometimes including their full names, family circumstances and telephone numbers. She even stated on the pages that one of her colleagues had injured her foot and was on half-time on medical grounds. Mrs Lindqvist had not informed her colleagues of the existence of the pages, or obtained their consent. She was prosecuted for breaching the Swedish legislation that implemented the DPD into Swedish law, and convicted on first instance for *inter alia* trans-
ferring processed data to a third country without authorisation. On appeal, reference was made for guidance of the CJEU.\textsuperscript{78}

One of the questions referred, which is of relevance here, was question five, where the CJEU was asked to address the ‘transfer’ issue and assess whether Lindqvist’s conduct meant that she had transferred data to a third country:

\textit{Directive 95/46 prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden – with the result that personal data become accessible to people in third countries – does that constitute a transfer of data to a third country within the meaning of the Directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?}\textsuperscript{79} (emphasis added)

In short, the Court found that there is no transfer of data to a third country within the meaning of Article 25 of the Directive when an individual in a member state loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person established in that State or in another member state, thereby making those data accessible to anyone who connects to the Internet, including people in a third country.\textsuperscript{80}

\textsuperscript{78} C-101/01 (Lindqvist), paragraphs 15-18.
\textsuperscript{79} C-101/01 (Lindqvist), paragraph 18.
\textsuperscript{80} C-101/01 (Lindqvist).
3.3 The Court’s justification

3.3.1 The first justification

The Court gave three grounds for its conclusion. After noting the necessity of taking account both of the technical nature of the operations carried out and of the purpose and structure of Chapter IV of the Directive where Article 25 appears, the Court took account of the technical setup in question. It observed that in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to connect to the Internet, but also carry out the necessary actions to consult those pages. Therefore, Mrs Lindqvist’s internet pages did not contain the technical means to send the information automatically to people who did not intentionally seek access to those pages. Consequently, any transfer of data that took place was through the computer infrastructure of the hosting provider where the page was stored. In other words, the Court’s first justification was that no direct transfer had taken place between the person who accessed the data from a third country and the person who uploaded that data to an internet page, even though the data was made accessible on the pages. The users themselves had to carry out the necessary actions to access the information and thus, no data was sent automatically from the server to the users.

This first justification has been criticised for taking into account considerations that seem irrelevant, such as whether or not the data were actually accessed outside the EU/EEA. The Court should rather have asked the key question of whether the data could have been accessed. A failure to count as transfers of data situations where the data is not automatically transmitted to countries seems unsound, as there may be just as much intention to make data available to other countries where it is merely made accessible, as when they are actively transmitted.

81 C-101/01 (Lindqvist), paragraph 57.
82 C-101/01 (Lindqvist), paragraph 60-61.
83 Kuner, Transborder Data Flows and Data Privacy Law, 13.
Another criticism that has emerged, is that there is no difference between the facts at stake in *Lindqvist* and the fact that a TV station cannot provide TV programs to somebody who does not turn on their TV or choose a particular TV channel. In this sense, it is probable that new technological developments will blur the distinction between automatic transmission and active transmission to a point where it can no longer be maintained. The first justification, by reference to the relevant technology, has thus been criticised for being weak. 84

### 3.3.2 The second justification

The Court’s second justification related to the purpose of chapter IV of the Directive. After observing that Chapter IV contains no provision concerning use of the Internet, the court argued that in light of the state of the development of the Internet at the time the Directive was enacted, it could not be presumed that it was the legislator’s intention to encompass website publishing by an individual, as in the case of *Lindqvist*, within the expression of 'transfer [of data] to a third country’. 85

This justification has also been criticized for being weak, as the fact that the Directive does not contain any provision relating to the use of the Internet suggests that the language of the Directive is technology neutral, and that it should thus be applied independently of the technology in question. Thus, it cannot be presumed that the legislator’s intention was that it should not apply to internet-related activities. If that were the case, the drafters of the Directive would presumably have made that clear, especially in light of the fact that the Internet was in place at the time the Directive was drafted. 86

---


85 C-101/01 (*Lindqvist*), paragraphs 67-68.

86 Svantesson, “Privacy, Internet and Transborder Data Flows,” 15.
3.3.3 The third justification

The third justification for the Court’s decision has gotten more support from scholars and is seen as the most convincing one and even praiseworthy for taking into account the international implications of the decision.\(^{87}\) The third justification was based on the likely consequences it would have if to conclude otherwise, namely that finding that transfer of data had taken place in this case would make the entire Internet subject to European data protection law\(^{88}\):

> If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the Internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the member states would be obliged to prevent any personal data being placed on the internet.\(^{89}\) (emphasis added)

Further, the Court found it unnecessary to investigate whether an individual from a third country had accessed the internet pages in question, or whether the server of the hosting

---

\(^{87}\) Bygrave, Data Privacy Law, 192, Kuner, Transborder Data Flows and Data Privacy Law, 13 and Svantesson, “Privacy, Internet and Transborder Data Flows,” 16.

\(^{88}\) Kuner, Transborder Data Flows and Data Privacy Law, 12.

\(^{89}\) C-101/01 (Lindqvist), paragraph 69.
service was physically located in a third country, considering that the operations carried out by Mrs Lindqvist did not, as such, constitute a transfer of data to a third country.  

This type of argument illustrates that the Court not only applied the law to the situation at hand, but made in fact an assessment of the likely consequences of finding that Mrs Lindqvist’s conduct constituted a transfer. By doing so, the Court took into account the legal issues that arise with technologies that are rapidly developing. Therefore, this argument is almost impossible to dismiss, even though it might be difficult to argue that Mrs Lindqvist’s conduct did not amount to a transfer, as the consequences of concluding otherwise would be devastating for the technology in question. In that sense, it may be said that the Court applied a reasonableness test, by taking into account the consequences of reaching a contrary conclusion.

3.4 Implications

3.4.1 Introduction

There continues to be a lack of clarity regarding what constitutes ‘transfer’ of data following the Lindqvist decision, as the Court seemed to base its decision on certain case-specific technical factors relating to how the data were accessed on the Internet. Further, it might be the case that the decision was motivated in part by a desire to remedy the specific situation of Mrs Lindqvist. The implications of Lindqvist for clarifying what constitutes ‘transfer’ of data are therefore to some extent limited. This applies both to situations where individuals and companies upload their personal data to the Internet.

---

90 C-101/01 (Lindqvist), paragraph 70.
91 Svantesson, “Privacy, Internet and Transborder Data Flows,” 16.
92 Further elaborated upon in chapter 3.4.2.
93 Kuner, European Data Protection Law, 81-82.
The Court left some questions unanswered by not addressing the status of certain parameters by which data is disseminated on the Internet and related platforms. Most notably the Court did not address whether the location of the server(s) of the hosting provider matters, and whether the type of access to data that is given to parties in third countries matters. This second parameter may be specified further by asking whether transfer of data takes place when access is provided intentionally by the uploader, but restricted to predefined persons or organizations. Uncertainties regarding these parameters are unfortunate, in light of the enormous increase of cloud computing services and online social networks that has emerged since the Lindqvist decision was handed down.  

With that being said, the following discussion will address the extent the Lindqvist decision does provide guidance as to what constitutes ‘transfer’ of data, by applying the criteria provided in Lindqvist to the aforementioned parameters, to the extent possible. Before addressing those issues, an overview of the technical factors seemingly decisive for the Court’s decision in Lindqvist will be provided, and their effect for the decision’s implications for other scenarios discussed.

### 3.4.2 Technical factors

The Court seemed to base its decision on a number of specific technical factors that may limit the decision’s applicability and implications for other scenarios. These factors are firstly the fact that there was no evidence of actual transmission of the data to persons outside the EU; secondly that the data were all in Swedish and thus not targeted towards persons outside the EU; and thirdly that the data were designed to be accessed on a limited scale by a small number of persons. Since these factors are case-specific, it may not be assumed that the decision provides a wide loophole for companies to avoid the application

---


95 Kuner, *European Data Protection Law*, 82 and 156.
of the transfer restrictions in the Directive by using server(s) in the EU/EEA to host global databases and make them accessible via the Internet.\textsuperscript{96}

Further, the \textit{Lindqvist} decision implies that transfer of data should be an \textit{active act} that involves sending data, but not making the data passively accessible.\textsuperscript{97} This does however not mean that granting access to data may under no circumstances constitute 'transfer’ of data. In light of all this, some scholars are of the opinion that the safest interpretation of \textit{Lindqvist} is that making personal data available on the Internet can be viewed as transfer of data, given that it involves granting access to data about other parties (for example employees, customers, etc.) on a \textit{large scale} and for \textit{business purposes}. Under this interpretation, a company that places large amounts of data on the Internet and makes it accessible to a large number of employees or contractors on a global scale would most likely be deemed to have transferred the data in question, and have to comply with all applicable legal restrictions regarding transfers of data.\textsuperscript{98}

\subsection*{3.4.3 Consequences}

Despite the uncertainties that remain following \textit{Lindqvist}, the decision does nevertheless provide some criteria that may be useful when determining whether 'transfer’ of data has occurred or not. Those criteria are firstly the 'direct transfer'\textsuperscript{99} requirement and secondly the 'reasonableness test'\textsuperscript{100} approach. The following discussion will assess to which extent these criteria have implications for the definition of ‘transfer’ by discussing the extent to which they can be applied to the parameters mentioned in chapter 3.4.1.

\begin{itemize}
\item Kuner, \textit{European Data Protection Law}, 156.
\item C-101/01 (\textit{Lindqvist}), paragraphs 60-61.
\item C-101/01 (\textit{Lindqvist}), paragraphs 60-61.
\item \textit{C-101/01 (Lindqvist)}, paragraph 69 and Svantesson, “Privacy, Internet and Transborder Data Flows,” 16.
\end{itemize}
3.4.3.1 Location of server(s)

Turning to the parameter of whether the location of the server(s) matter, Lindqvist does at first sight suggest that if an individual uploads personal data to a hosting provider established within the EU/EEA, that such acts do not constitute 'transfer' of data, irrespective of the location of the server(s).\(^{101}\)

Such an approach does however not take into account the Court’s strongest argument relating to the consequences of finding that 'transfer' of data had taken place. The acts carried out by Mrs Lindqvist could have been considered as 'transfer' if not for the devastating consequences for the technology in question, namely that the provisions of Chapter IV of the Directive would then become of general application to the entire Internet (reasonableness test').\(^{102}\) Thus, if there had been proof of a grant of actual access, 'transfer' should have been deemed to have taken place, regardless of the location of the server(s), given that the 'reasonableness test' had been fulfilled.\(^{103}\)

In light of this, I am of the opinion that a controller that uploads personal data to a provider established within the EU/EEA, that uses server(s) located within that area, cannot rely on their location as a safeguard for preventing that any 'transfer' of data takes place. The reason for this is that it is possible to find that 'direct transfer'\(^{104}\) to a person or a company in a third country has taken place, if the consequences of finding that 'transfer' of data has taken place do not make Chapter IV of the Directive of general application to the entire Internet.\(^{105}\)

\(^{101}\) C-101/01 (Lindqvist), paragraphs 67 and 70 and Hon and Millard, “Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA?”, 9-10.

\(^{102}\) C-101/01 (Lindqvist), paragraph 69 and Svantesson, “Privacy, Internet and Transborder Data Flows,” 16.

\(^{103}\) Esayas, “A walk in to the cloud and cloudy it remains,” 669.

\(^{104}\) C-101/01 (Lindqvist), paragraphs 60-61.

\(^{105}\) C-101/01 (Lindqvist), paragraph 69 and Svantesson, “Privacy, Internet and Transborder Data Flows,” 16.
Turning to server(s) located outside the EU/EEA, the question to ask is whether 'transfer' takes place by the act of uploading data to such servers, or whether it is possible to argue, based on Lindqvist, that no 'transfer' of data occurs even if the server(s) are located in a third country?

The A29WP is of the opinion that when an ad network provider uploads data to servers located in third countries, such actions shall be considered as 'transfer' of data within the meaning of the Directive. At the same time, in Lindqvist, the Court found it unnecessary to investigate whether the server in question was physically located in third country, although it recognised that the hosting provider’s infrastructure might be located in other countries. In this context the Court stressed that its answer only related to the uploader’s activities (those of Mrs Lindqvist), and not those carried out by the hosting providers.

This does indeed suggest that whether 'transfer' of data takes place or not is independent of the location of the server(s), but rather depends on the 'direct transfer' requirement and the 'reasonableness test'. Lindqvist thereby suggests that the location of the server(s) is not decisive for determining whether 'transfer' of data occurs. This may further be supported by the fact that the Court did not take the location of the server into account when assessing whether 'direct transfer' had taken place; that is, whether data had actually been received in a third country.

The conclusion regarding the implications of Lindqvist for the parameter of whether the location of servers matters when determining whether 'transfer' of data occurs or not, is therefore negative for the instances where a controller uploads data to a hosting or a

106 Article 29 Working Party, “Opinion 2/2010 on online behavioural advertising,” 21, stating that “if the data is transferred outside the EU, for example to servers located in third countries, ad network providers must ensure compliance with the provisions on transfers of personal data to third countries.”
107 C-101/01 (Lindqvist), paragraph 70.
108 C-101/01 (Lindqvist), paragraph 62.
network provider that uses servers in a third country. This is due to the fact that the transfer takes place through the "computer infrastructure of the hosting provider" \(^\text{109}\) and not by the acts of the controller. However, if the controller uploads the data to servers located in a third country himself, or if the controller is a hosting or a network provider himself, then his actions are deemed to constitute 'transfer' of data within the meaning of the Directive, according to Lindqvist. And it may be added that a provider might risk becoming a controller through a decision to use a non-EU/EEA servers. \(^\text{110}\)

3.4.3.2 Type of access

Turning to the parameter of whether the type of access to data that is given to parties in third countries matters, the focus will be on the aspect of whether 'transfer' occurs when access is provided intentionally by the uploader, but restricted to predefined persons or organizations.

Under the aforementioned 'safest interpretation' of Lindqvist, making personal data available on the Internet can be viewed as 'transfer' of data, given that it involves granting access of the data of other parties on a large scale and for business purposes. \(^\text{111}\) The interpretation presumably excludes situations where individuals upload personal data about their 'friends' to online social network. However, it has been asserted that when an individual uploads personal data to an online social network with the intention of making the information publicly accessible by extending access to their network to the public, that such actions may constitute 'transfer' of data within the meaning of the Directive. \(^\text{112}\)

\(^{109}\) C-101/01 (Lindqvist), paragraph 61.

\(^{110}\) Hon and Millard, “Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA?”, 10.

\(^{111}\) Kuner, European Data Protection Law, 82 and 156.

The question to ask then is if, in light of *Lindqvist*, the fact that an *intention* exists to make the data accessible would be decisive for determining whether 'transfer' of data has occurred or not, regardless of the 'direct transfer’ requirement and the 'reasonableness test’? More specifically, would the act of intentionally providing restricted access to the data to predefined persons or organizations constitute 'transfer’ of data? The core of this question is whether it is possible to read from *Lindqvist* that whether 'transfer’ takes place or not is dependent of the intention to make the data accessible. And if so, what would constitute such intention?

Regarding cloud computing, it has been argued based on *Lindqvist*, that if a controller uploads personal data to a cloud provider established within the EU/EEA, with the intention to store or operate the data, but not to make it accessible, that the controller does not 'transfer’ the data. This applies even if the cloud provider uses non-EU/EEA data centres to provide its services.\(^{113}\) This suggests that *Lindqvist* applies to situations where intention to make the data accessible is absent, and not to situations where such intention exists.\(^{114}\)

From this interpretation it follows that in situations where intention to provide access to the data is absent, that the criteria established in *Lindqvist* ('direct transfer’ requirement and the 'reasonableness test’) must be fulfilled in order to find that 'transfer’ has taken place. It also follows that in situations where intention to make the data accessible to persons or organizations in third countries exists, that 'transfer’ should be deemed to take place in such circumstances, regardless of the 'direct transfer’ requirement and the 'reasonableness test’.\(^{115}\)

---

\(^{113}\) Hon and Millard, “Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA?”, 10.

\(^{114}\) Esayas, “A walk in to the cloud and cloudy it remains,” 670.

\(^{115}\) This is supported by the UK Information Commissioner’s Office (hereinafter 'ICO’), which is UK’s DPA, that considers that if a controller uploads data to the Internet with the intention that it be accessed in third
This may further be supported by the consideration that it would be contradicive to count as 'transfers' of data cases where data is transferred to a specific organization in a third country or an individual, but not cases where data is made accessible for the whole world with that exact purpose. This would namely create an opportunity for a circumvention of the provisions by legalizing the cases where the data is accessible worldwide.\textsuperscript{116} Thus, providing restricted access intentionally to predefined persons or organizations in third countries should also be deemed to constitute 'transfer' of data within the meaning of the Directive, given that the entity that provides access to the data is the controller of the data.\textsuperscript{117} The prerequisite for such a finding is however that the access is provided intentionally. Where such intention exists, it justifies assessing the level of protection guaranteed by the recipients’ country and other possible measures to be taken in order to protect the data.\textsuperscript{118}

The reply to the question of whether the type of access to data that is given to persons in third countries matters, is therefore positive, as if access is provided intentionally, it should be deemed to constitute 'transfer' of data within the meaning of the Directive. The challenge that remains is how to determine such an intention.

If a controller has knowledge that his hosting provider uses servers located outside the EU/EEA, does that constitute intention to make the data accessible in third countries? Should the controller be responsible for making inquiries regarding the server’s location? Could a lack of inquiry be interpreted as an intention to make the data accessible in third

\textsuperscript{116} Esayas, “A walk in to the cloud and cloudy it remains,” 670.
\textsuperscript{118} European Data Protection Supervisor, “Opinion of the European Data Protection Supervisor on the data protection reform package,” 19.
countries? And further, must the controller assess the extent the provider’s ability to access its data? The Lindqvist decision does not answer these questions, but due to their importance they will be reflected upon in chapter six.

However, based on Lindqvist, what can be asserted is that uploading of data onto servers outside the EU/EEA and intentionally providing access to such data to a person or an organization in a third country would in any case constitute ’transfer’ of data to a third country.

4 National law

4.1 Introduction

In this chapter, I will take a look at national laws of selected countries and their approach to define (or not to define) the concept of ’transfer’ of data. Focusing on Norway, I will start by assessing with a critical eye, how the DPD has been implemented into the PDA. I will moreover look at the Norwegian DPAs approach to the matter, relevant decisions of the Norwegian Privacy Appeals Board and commentaries by scholars. Following that, I will assess how Germany has defined the concept and then turn to United Kingdom and Australia and look at their approaches. Finally, I will give a short summary in the end of chapter four, where I will consider these various approaches, but I will analyse the guidance they provide in chapters five and six.

Hon and Millard, “Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA?”, 10-11.
4.2 Norway

4.2.1 The Norwegian PDA

In the PDA, the concept 'transfer' of data is not defined. However, the concept 'processing of personal data' is defined in PDA section 2(2) as "any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses", while 'processor' is defined in PDA section 2(5) as "the person who processes personal data on behalf of the controller". What is worth criticising in this context is that the PDA fails to implement adequately the Directive’s definition of the concept of 'processing' by not explicitly stating that it encompasses 'disclosure by transmission, dissemination or otherwise making available'.\[120\] Whether or not the term 'disclosure' is supposed to encompass such acts is unclear, as it is not explicitly stated in the provision, which creates unclarity for controllers established in Norway.

Turning to chapter V of the PDA, which implements Chapter IV of the Directive and regulates transfer of personal data to other countries, the focus will be on criticising the way Article 25(1) of the Directive has been implemented in PDA section 29(1). Before analysing PDA section 29(1), it is worth noting that PDA sections 29(2) and 30 have implemented Articles 25(2) and 26 of the Directive in a way almost identical to the conditions set out in the Directive. Thus, those provisions will not be subject to a criticism in this chapter.

PDA section 29, which sets out the basic conditions for transfer, reads as following: "Personal data may only be transferred to countries which ensure an adequate level of protection of the data. Countries which have implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data meet the requirement as regards an adequate level of protection.” What is worth noting is that this provision leaves out certain specific conditions explicitly stated

\[120\] See Article 2(b) of the Directive.
in Article 25(1) of the Directive, namely that the provision applies to data which are *undergoing processing* or are *intended for processing after transfer*.

In other words, PDA section 29(1) leaves out an essential part of DPD Article 25(1) by leaving out that the provision applies to personal data which are undergoing processing or are intended for processing after transfer. Doing so may leave controllers established in Norway in an uncertainty regarding which situations require compliance with PDA section 29(1).

Turning to the preparatory works to the PDA, one point assessed was the concept of 'transfer' of data in relation to use of the Internet and related platforms.\textsuperscript{121} The point of departure taken was that every single communication form must be assessed when determining whether or not it constitutes 'transfer' of data within the meaning of the Act. It was noted that many of the websites established on the Internet will normally fall outside the scope of the Act, as they will often be purely private or include data about products without including any personal data. For the websites that fall within the scope of the Act, it would be natural to define publishing on such websites as 'transfers' of data to a third country. The reason for this is that when data is first made accessible, there is a great chance that they will also be downloaded and used in a third country. The sending of an email through the Internet should also be seen as 'transfer' of data if the recipient is located in a third country. However, if the recipient is located in Norway, the use of the email should not be seen as transfer, even if the email technically routes through a third country on its way to Norway.\textsuperscript{122}

The Justice Committee agreed with this view, but pointed out that the use of the Internet and related platforms would create many new challenges for the law in the future, and that this field would have to be followed up closely in the future. The Committee thus

\textsuperscript{121} Ot.prp. nr. 92 (1998-1999), 74-75.
\textsuperscript{122} Ot.prp. nr. 92 (1998-1999), 74-75.
presupposed that this question would be presented for the Norwegian Parliament (Stortinget) again later on.\textsuperscript{123}

### 4.2.2 The Norwegian DPA and the Norwegian Privacy Appeals Board

The Norwegian DPA has published a guidance on 'Transfer of personal data to third countries’, but the part relating to the question of what constitutes ‘transfer’ of data to a third country is very brief. According to the guidance, the provisions on transfer of data to a third country only apply to transfer of personal data to an address in a third country. Information uploaded on the Internet that can in principle be read by all, will as a rule not fall under the strict conditions that apply to transfers of data to third countries. That kind of publishing will fall under other provisions.\textsuperscript{124}

Further, the guidance provides that if one sends an email to a recipient in a third country, such an act constitutes ‘transfer’ of data to a third country. On the other hand, if one sends an email to a recipient in Norway, that will not constitute ‘transfer’ of data, even though the email routes through a server in a third country on its way.\textsuperscript{125}

Turning to the Norwegian Privacy Appeals Board, it has not provided a thorough guidance through its practice regarding what constitutes ‘transfer’ of data within the meaning of the PDA. What is of interest however, are the so-called ‘GE cases’\textsuperscript{126}, which all related to the same issue, namely unauthorized retrieval of health data through a vendor’s (GE) remote access.

\textsuperscript{123} O. nr. 51 (1999-2000), chapter 10.
\textsuperscript{124} Datatilsynet, ”Overføring av personopplysninger til utlandet.”
\textsuperscript{125} Datatilsynet, ”Overføring av personopplysninger til utlandet.”
\textsuperscript{126} PVN-2013-05, 08, 09, 11 and 12 and PVN-2014-22 and 24.
In these decision of the Norwegian Privacy Appeals Board, it confirmed the Norwegian DPA’s understanding that when a vendor, responsible for maintenance and surveillance of medical equipment, retrieves personal data (in this case, sensitive personal data) through a remote access from companies, and transfers the data to an information system in USA, that ’transfer’ of data within the meaning of the PDA has taken place.\textsuperscript{127}

\subsection*{4.2.3 Commentaries by scholars}

The Norwegian scholar Jarle Roar Sæbø has addressed how to define the concept of ’transfer’ of data, from the standpoint of outsourcing. Focusing on whether making data accessible to persons in third countries constitutes ’transfer’, he addressed specifically whether it matters whether those persons have in fact accessed the data or not. In his opinion, transfer does not have to be permanent to occur, and can take place even if it is deleted from a storage medium\textsuperscript{128} in a third country after a short period of time.\textsuperscript{129}

Regarding whether it is sufficient that persons in third countries have access to the data without in fact accessing them, Sæbø asked the Norwegian DPA in 2013 for a statement regarding whether such acts constitute ’transfer’ of data.\textsuperscript{130} The Norwegian DPA’s reply was negative.\textsuperscript{131} However, in Sæbø’s opinion the data should nevertheless be protected adequately in order to avoid carrying out illegal transfers of data, if someone in the third country in fact accesses the data.\textsuperscript{132} Finally, he notes that due to constantly new technologies, new variants of the question of what constitutes ’transfer’ of data are

\textsuperscript{127} PVN-2013-05, 08, 09, 11 and 12 and PVN-2014-22 and 24.
\textsuperscript{128} Even if it is a storage medium used for temporary storage.
\textsuperscript{130} The statement regarded especially whether personal data is transferred within the meaning of the PDA when persons in a third country have a reading access to a storage solution where personal data is stored, but given that they have not made use of the reading access, in the context of outsourcing.
unavoidable. In such cases, one should use the PDA’s definitions of 'processing of personal data' and 'processor' cf. sections 2(2) and 2(5)\(^{133}\) to determine whether 'transfer' takes place. If a vendor of outsourcing services is located in a third country and is a 'processor' within the meaning of the Act, then 'transfer' of data takes place. This approach is however not confirmed by the Norwegian DPA, but gives in his opinion a good indication.\(^{134}\)

### 4.3 Germany

Even though neither the DPD nor the PDA provide a definition of the concept of 'transfer' of data, some member states’ national data protection laws do contain a definition of the concept. One of them is Germany, which defines 'transfer' in § 3(4)3 of the German Federal Data Protection Act as "the disclosure to a third party of personal data stored or obtained by means of data processing either a) through transmission of the data to the third party or b) through the third party inspecting or retrieving data held ready for inspection or retrieval."

### 4.4 United Kingdom

While Germany explicitly defines the concept of 'transfer’, that is not the case in the United Kingdom, as the UK 1998 Data Protection Act does not define the concept. However the UK ICO has issued a non-binding interpretative paper that provides some guidance regarding the concept of 'transfer’ of data.\(^{135}\)

After noting that the ordinary meaning of the word 'transfer' is transmission from one place, person etc. to another, the paper explicitly states that 'transfer' does not mean the same as 'mere transit’. Thus, instances where electronic transfer of personal data is routed

\(^{133}\) Along with other legal sources relating to these concepts.


\(^{135}\) UK ICO, "Data Protection Act 1998: The eighth data protection principle and international data transfers.”
through a third country on its way from the UK to another EU/EEA country does not constitute 'transfer' of data.  

Further, the paper explicitly explains that instances where information is provided by someone in the UK over a telephone to someone in a third country who then enters the information on a computer, is to be seen as 'transfer' of data that requires compliance with the UK Data Protection Act, as the data is intended for processing after transfer. Moreover, the paper refers to Lindqvist and asserts that the principles of that case do not apply to cases where data is loaded onto the Internet with the intention that the data be accessed in a third country. Such actions will thus usually constitute 'transfer' of data.

4.5 Australia

4.5.1 Introduction and issues assessed

In Australia, the concept of 'transfer' is not defined as of today. What is of interest however, is that an inquiry was conducted by the Australian Law Reform Commission (hereinafter 'ALRC'), relating to the extent to which the Australian Privacy Act 1998 and related laws continue to provide an effective framework for the protection of privacy in Australia. This inquiry resulted in the 'ALRC Report 108' published in 2008, and one of the aspects assessed in the Report was the 'definition of transfer', which will be the focus of this subchapter.

_____________________

139 Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108)."
In its Report, the ALRC examined whether it would be useful to distinguish the term ‘transfer’ from the terms ‘use’ and ‘disclosure’. One way of doing that would be to define the concept of ‘transfer’ in the Australian Privacy Act to include situations where data is stored in Australia but accessible or viewable from outside Australia. Including such situations would include uploading data to the Internet. The ALRC thus asked whether or not a definition of ‘transfer’ should include cases where personal data is stored in Australia in a way that allows it to be accessed or viewed outside Australia.\(^{140}\)

Another aspect assessed by the ALRC was whether a potential definition of ‘transfer’ should encompass situations where emails containing personal data are sent by or to email systems hosted overseas. An example of this is where a doctor in Australia emails some test results to an Australian patient, via an email containing sensitive personal data, stored on a server overseas. Would such acts constitute ‘transfer’ of data to someone in a foreign country? ALRC’s point of departure was that the answer would seem to be yes, as the information would be placed on a server located in a foreign country. The question thus asked was whether a definition of ‘transfer’ should exclude temporary transfers of personal data, given that the data had not been viewed outside Australia.\(^{141}\)

4.5.2 Assessment

These questions received a wide range of views from different stakeholders. Some agreed with ALRC’s proposed definition of the term, while others did not. Some agreed in part and were of the view that the term ‘transfer’ should indeed be defined, but should not


exclude cases where data was transferred overseas by accident because the entity sending the data had not taken reasonable steps to protect the data.\textsuperscript{142} Other stakeholders disagreed and argued that a concept such as 'transfer' of data would become even more difficult to define as emerging technologies would further blur the question of where data is stored and the distinction between permanent and temporary copies of data.\textsuperscript{143}

Regarding the question of whether the term 'transfer' should encompass circumstances where personal data is stored in Australia in a way that allows it to be accessed or viewed outside Australia, no consensus from stakeholders was reached. Some of them supported its inclusion, while others argued that transfer would not occur merely due to the fact that it was possible that the data would be accessed or viewed outside Australia, but only if that actually occurred. Other stakeholders opposed the inclusion of this in the definition.\textsuperscript{144}

Turning to the question of whether 'transfer' should exclude temporary transfers of personal data, there was also a lack of consensus among stakeholders. Some stakeholders supported its exclusion, and argued that such transfers should fall outside the scope of regulation, as compliance costs regulating them would by far outweigh the privacy-related interests in question. Others were of the opinion that communication of data by routes that enable it to be intercepted by parties outside Australia should constitute 'transfer' of data.\textsuperscript{145}

\begin{itemize}
\item \textsuperscript{142}Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108)," paragraphs 31.185-6.
\item \textsuperscript{143}Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108)," paragraph 31.187.
\item \textsuperscript{144}Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108)," paragraph 31.188-9.
\item \textsuperscript{145}Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108)," paragraph 31.190-1.
\end{itemize}
In light of all this, the ALRC noted that a high level of complexity is attached to the way in which personal data is transferred. It added that if personal data is stored in Australia, but viewed or accessed outside Australia, it should be deemed to be 'transfer’ of data. If personal data is routed and stored temporarily outside Australia, but not accessed, it should not be seen as constituting 'transfer’ of data. If it were accessed however, it should constitute 'transfer’ of data. 146

4.5.3 ALRC’s conclusion

With all these considerations taken into account, the ALRC came to the conclusion that providing a definition of 'transfer’ is not likely to clarify the situation, especially in light of the rapid advances in technology and the difficulties associated with distinguishing between permanent and temporary storage of data. The ALRC’s conclusion was thus that the term 'transfer’ should not be defined in the Australian Privacy Act. Rather, the question should be resolved on a case-by-case basis, with assistance from the OPC Guidance. 147

The OPC Guidance relates to cross-border data flows and the ALRC noted that it should provide examples of circumstances where transfer would, or would not, be deemed to take place. The reason for this being the ALRC’s preferred approach was that the Guidance could be more easily be amended to accommodate changes relating to the ways in which personal data is transferred, due to emerging technologies, than providing a definition of the concept of ‘transfer’. 148

4.6 Summary and consideration

The above assessment shows that the chosen countries have approached the concept ‘transfer’ of data in various ways.

The Norwegian approach seems to be the weakest of all the aforementioned approaches. Not only does the PDA fail to adequately define essential concepts such as ‘processing of personal data’ and ‘processor’\textsuperscript{149}, but it also fails to mention that PDA section 29(1) applies only to data which are “undergoing processing or intended for processing after transfer”, cf. Article 25(1) of the Directive.

Further, what may be read from the preparatory works to the PDA and the DPA’s guidance\textsuperscript{150}, is that ‘mere transit’ of data, i.e. when data is for example sent from Norway to another EU/EEA member state but is routed through a third country on its way, does not constitute ‘transfer’ of data. However, the preparatory works to the PDA and the DPA’s guidance provide different answers regarding whether publishing data on the Internet constitutes ‘transfer’ of data. That issue remains thus questionable. However, in light of the DPA’s statement regarding outsourcing, it may be asserted that providing access to data to persons in third countries, without the data ever being accessed, does not constitute ‘transfer’ of data. I am of the opinion that the Norwegian PDA creates unnecessary uncertainty for controllers, especially the ones established in Norway, and that it ought to be amended in order to adequately implement the aforementioned provisions of the Directive. Doing so would at least make it easier to distinguish between acts that constitute ‘transfer’ of data and those that do not.

Turning to Germany, the definition of ‘transfer’ under § 3(4)3 of the German Federal Data Protection Act seems to encompass both cases where data is made available to third parties

\textsuperscript{149} See Articles 2(b) and 2(e) of the Directive and PDA sections 2(2) and 2(5).

\textsuperscript{150} See Ot.prp. nr. 92 (1998-1999), 74-75 and Datatilsynet, “Overføring av personopplysninger til utlandet.”
for view or access, cf. the wording "inspecting or retrieving data". The definition furthermore suggests that an intention to disclose the data to a third party must exist in order for 'transfer' to take place, cf. the wording "through transmission [...] to a third party", and "held ready for inspection or retrieval". I am of the opinion that the German definition of 'transfer' requires an intention to transfer the data to a third party, even though it is not explicitly stated in the definition.

What may be read from the UK ICO’s approach\textsuperscript{151}, is that the act of providing access intentionally to parties in third countries constitutes 'transfer' of data within the meaning of the UK 1998 Data Protection Act, that requires compliance with the Act. 'Mere transit' is not seen as 'transfer' of data, given that the data is routed through a third country on its way to a member state of the EU/EEA. And finally, the act of providing information through for example a telephone, and then entering that same information on a computer, is to be seen as 'transfer' of data, as the data is intended for processing after its transfer. I am of the opinion that the UK ICO’s approach is a good example of how a guidance from a DPA can provide legal certainty and clarify to a great extent what constitutes 'transfer' of data.

In the Australian Privacy Act, the concept of 'transfer' of data is not defined. The reasons for the ALRC’s conclusion of not defining the concept, after viewing a wide range of views from stakeholders, was that doing so would not be likely to clarify the situation. Special attention was given to the rapid advances in technologies and the difficulties associated with distinguishing between permanent and temporary storage of data. The preferred approach taken was that the question should be resolved on a case-by-case basis, with assistance from the OPC guidance, which could more easily be amended in order to

\textsuperscript{151} See UK ICO, "Data Protection Act 1998: The eighth data protection principle and international data transfers", 5.
accommodate changes relating to the ways in which data is transferred.\textsuperscript{152} I am of the opinion that the Australian approach provides a solution that is better than not providing any guidance regarding what constitutes ’transfer’ of data, as is the case at a European level as of today. However, such an approach should not be accepted unless a certain guidance providing examples of what constitutes ’transfer’ of data is in place.

In this chapter, I have assessed the national laws of selected countries and their approach to define, or not to define, the concept of ’transfer’ of data. Even though these approaches vary, they do provide certain elements that are worth taking into account when determining if, and then how, the concept of ’transfer’ of data is to be defined under European data protection legislation. I will assess the implications of these elements further in chapters five and six.

\section{5 De lege ferenda}

\subsection{5.1 Introduction}

In this chapter I will address whether the concept of ’transfer’ of data ought to be defined, preferably in the GDPR, by discussing \textit{de lege ferenda}. Today, the concept is not defined in the draft to the GDPR. In order to assess this, I will go through the pros and cons of defining the concept. I will also assess whether the concept of ’mere transit’ should be distinguished from the term ’transfer’ of data.

\subsection{5.2 Disadvantages of defining the concept ’transfer’ of data}

Possible disadvantages of defining the concept of ’transfer’ of data are first of all that advances in technology are nowadays so rapid, that it may be hard to define the concept in

\footnote{\textsuperscript{152} Australian Law Reform Commission, ”For Your Information: Australian Privacy Law and Practice, (ALRC Report No 108),” paragraph 31.193.}
a way that is satisfyingly technology neutral, as it may be hard to grasp all the potential changes relating to the way in which data is transferred. This argument is well illustrated in ALRC’s report, as discussed in chapter 4.5, as was one of the main arguments for the ALRC’s conclusion for not defining the concept.\textsuperscript{153}

A second possible disadvantage of defining the concept is directly related to the first disadvantage, namely that due to emerging technologies, the question of where data is stored and the distinction between permanent and temporary copies of data gets further blurred. This was another of the main arguments for the ALRC’s conclusion for not defining the concept of ‘transfer’.\textsuperscript{154}

A third possible disadvantage of defining the concept is that if one would exclude circumstances where data is stored in an EU/EEA member state, but made accessible to persons in third countries, without being in fact accessed, there is as risk that the data could nevertheless be accessed or downloaded by parties in third countries. Excluding such scenarios from the scope of the concept ‘transfer’ of data, could thus create certain risks, unless some technical measures are taken that prevent such access from taking place.

Finally, a fourth possible disadvantage of defining the concept is that it may be difficult to provide a definition that is not applicable to the Internet, as illustrated in Lindqvist. In this context, it is worth recalling that the Internet is structured to transit data and is based on technical parameters but not on geography, meaning that the actual route of the data may be unpredictable. Thus, defining when data is transferred across national borders is perhaps not feasible.\textsuperscript{155}

\textsuperscript{155} Kuner, Transborder Data Flows and Data Privacy Law, 6.
5.3 Advantages of defining the concept 'transfer' of data

Possible advantages of defining the concept 'transfer' of data are in my view, many. The main reasoning for defining the concept is, in my opinion, to provide a legal clarity. As my assessment shows, the lack of legal clarity creates unnecessary uncertainty in this field of law. Following Lindqvist, there continues to be a lack of clarity regarding certain aspects of the question of what constitutes 'transfer' of data, such as whether the location of server(s) matters, and whether the type of access to hosted data that persons in third countries are given, matters. Other aspects remain unclear as well, such as whether 'transfer' of data only takes place when it is actively transferred, or whether it is sufficient that it is passively made available to recipients located in third countries. Due to the immense development of various network environments in the years since the decision was handed down, these uncertainties as unfortunate. And in this context, it is especially unfortunate that the GDPR also does not define 'transfer'.

The EDPS supports this view, and has pointed out that it is problematic that the GDPR does not define 'transfer' of data, especially with regards to network environments, such as cloud computing, where data is not only being actively transferred, but also being passively made available to recipients located in third countries. This increases the lack of clarity regarding what constitutes 'transfer' of data. Therefore, the EDPS has called for a clear definition of the term 'transfer' in its Opinion on the data protection reform package.

---

156 Bygrave, Data Privacy Law, 191-192.
157 Kuner, Transborder Data Flows and Data Privacy Law, 11-12.
158 Bygrave, Data Privacy Law, 192.
In its Opinion, the EDPS notes that it remains unclear how far the CJEU’s reasoning in *Lindqvist* applies to exchange on networks other than publishing material on the Internet. Further, it puts forward elements which could contribute to identifying what constitutes ‘transfer’ of data. Among these are firstly whether the aim is to communicate the data to identified parties, rather than making it publicly available, as this justifies assessing the level of protection guaranteed by the recipients’ country and other possible measures to be taken in order to protect the data. The second element is whether the data has freely been made available with the aim of providing access to it, and the third element is whether it is likely that the transfer is actually going to be received by one or more recipients in third countries. Providing a definition of the concept of ‘transfer’ of data would likely provide a necessary clarity on this field of law, and thus make it easier for controllers to comply with applicable legal requirements in various network environments.

Secondly, knowing what constitutes ‘transfer’ of data is very important when determining whether restrictions under EU law on transferring personal data to third countries are applicable. This importance is increased by the fact that not only does ‘transfer’ of data require a legal basis under Chapter V of the GDPR, but it also constitutes a form of processing, which requires a legal basis, as mentioned in chapter one. Transferring data within EU/EEA member states or even within the same member state would thus also require a legal basis. Even though this paper focuses on ‘transfer’ of data outside the EU/EEA, this consideration must be taken into account when assessing whether or not the concept ought to be defined.

Thirdly, a lot of costs and efforts may be associated with complying with the legal requirements that apply when ‘transfer’ of data takes place. For example, in addition to the restrictions on transfer of data, some data protection laws require controllers to register the


’transfer’ with a DPA before they are carried out. This may not only involve substantial efforts, but can also impede or even slow down potential transfers of data.\textsuperscript{162} The risks of non-compliance are moreover higher in this area of EU data protection law, than in perhaps any other area, as restrictions on ‘transfers’ of data are taken very seriously both by data subjects and DPAs. Violations may thus have serious consequences.\textsuperscript{163} The risks of non-compliance decrease when no ’transfer’ takes place, as the restrictions on ‘transfer’ of data to third countries do not exist in such cases. Adding uncertainty regarding when these requirements must be complied with only increases the costs and efforts required to comply with them, and does in any case not increase the effectivity of businesses. It furthermore increases the risks of non-compliance with the restrictions.

Fourthly, the concept ought to be defined in order to adjust the European data protection legislation to the realities of modern technologies.\textsuperscript{164} In the past it was much easier to determine whether restrictions on ’transfer’ of data were applicable or not, as ’transfer’ was often accomplished by physical means that could easily be ascertained. With the emergence of the Internet and the constantly developing technologies the information age has brought so far, data is constantly being made accessible to third countries out of the EU/EEA through the Internet.\textsuperscript{165} As of today, uncertainty exists regarding whether uploading data to an Internet site, which can be accessed by a person in a third country, constitutes ’transfer’ of data or not. Would it be possible to argue that the EU legislators did not see any need for defining the concept at the time the Directive was enacted? Perhaps, but that would not explain why EU legislators have in the current draft to the GDPR decided not to define the concept. Furthermore, one should bear in mind that the Internet was in place at the time the Directive was drafted, though on a different scale.\textsuperscript{166} The need for defining the concept was

\textsuperscript{162} Kuner, \textit{Transborder Data Flows and Data Privacy Law}, 17.
\textsuperscript{163} Kuner, \textit{European Data Protection Law}, 152.
\textsuperscript{165} Kuner, \textit{European Data Protection Law}, 80.
\textsuperscript{166} Svantesson, “Privacy, Internet and Transborder Data Flows,” 15.
however clearly much less then than it is today, as technological developments have complicated the application of the restrictions on 'transfer' of data, which should take technology better into account.167

5.4 Should 'mere transit' be distinguished from 'transfer' of data?

Turning to the question of whether 'mere transit' should be distinguished from the term 'transfer', it may first be asserted that doing so would make it easier to define the circumstances that constitute 'transfer' of data. As previously noted, the point of departure is that when data routes through a non-EU/EEA member state when it is transferred from one member state to another, 'transfer' of data does not take place. This applies however only if the data in question are not processed during their presence in the non-EU/EEA country.168

Neither the Directive nor the GDPR define 'mere transit'. Article 4(1)(c) of the Directive excludes however the application of national law of an EU/EEA member state in certain cases. These cases are where equipment, located on the territory of a member state, is used by a controller not established within the EU/EEA, only in order to ensure transit through the EU/EEA territory. The policy behind this exemption is that the rights and freedoms of EU citizens are not affected in cases of 'mere transit'.169 In this context, it may be recalled that in the UK, distinction is drawn between 'transfer' of data and 'mere transit', defined as situations where data is routed through a third country on its way from the UK to another EU/EEA member state.170

168 Kuner, European Data Protection Law, 156.
169 Kuner, Transborder Data Flows and Data Privacy Law, 16.
The A29WP has defined 'transit' as circumstances where for example telecommunications networks (cables) only ensure that communications transit through the EU/EEA in order to reach third countries. Another example of 'transit' is when data routes on the Internet, consisting of a router finding the best path for a data packet to travel and then forwarding it on.\textsuperscript{171} The A29WP is of the opinion that the concept is to be interpreted narrowly, and points out that the simple point-to-point cable transmission is gradually disappearing and that telecommunication services increasingly merge pure transit with added value services.\textsuperscript{172}

I am of the opinion that the concept 'mere transit' should be distinguished from 'transfer' of data in the GDPR, given that 'transit' merely involves data being routed through a certain destination on its way to its final destination, and is not further processed during this transmission. It is hard to see how including 'mere transit' in definition of 'transfer' would protect the fundamental rights and freedoms of EU citizens, cf. Article 1(1) of the Directive and Article 1(2) of the GDPR. The fact that data is in mere transit means that data is only being passed on from one connection point to the next, and this form of processing does not in itself pose any risk to the data.\textsuperscript{173} Moreover, as the purpose of the transit is not to process the data, and no intention exists to make them accessible to persons in third countries, it may be asserted that all of these factors argue against including 'mere transit' in the definition of 'transfer' of data. Further, the consequences of including 'mere transit' in the definition, would not only result in more uncertainty, but it would be practically impossible to determine the actual route of the data. This is due to the architecture of the Internet. Distinguishing between these concepts would also help defining what constitutes


\textsuperscript{172} Article 29 Working Party, "Opinion 8/2010 on applicable law," 23.

\textsuperscript{173} Kuner, \textit{Transborder Data Flows and Data Privacy Law}, 175.
’transfer’ of data. Further, the costs of regulating ’mere transit’ by far outweigh the privacy interests of regulating them.\textsuperscript{174}

In light of all this, I am of the opinion that the criteria that should be applied when distinguishing between ’mere transit’ and ’transfer’ of data is whether the data is simply being passed on to the next connection point, and whether the data is not further processed during its transit. If the answer is positive to both of these questions, then the transit should not be deemed to constitute ’transfer’ of data.

5.5 Summary

In this chapter, I have assessed the disadvantages and advantages of defining the concept of ’transfer’ of data. In light of all these factors, I am of the opinion that the advantages of defining the concept outweigh the disadvantages of doing so. I am strongly of the opinion that ’mere transit’ should be distinguished from the concept of ’transfer’ of data, given that it is not further processed during its transit, as the privacy-interests of data subjects would not be served by doing so. As I’ve come to the conclusion that the concept of ’transfer’ of data should be defined, I will suggest how the concept could be defined in the next chapter.

6 Conclusion

In this chapter, I will draw a conclusion as to how and when ’transfer’ of data takes place and suggest how the concept could be defined, in light of a holistic analysis of all the aforementioned factors. In order to do so, I will discuss factors that should be decisive when defining the concept. As discussed in chapters 5.4 and 5.5, ’mere transit’ should be distinguished from the concept ’transfer’ of data, for the reasons outlined above.

As a starting point, a definition of 'transfer' of data, that is dependent on the state of technology at a particular time, would quickly become outdated, due to the rapid advances in technology. Instead of referring to certain technical methods in which 'transfer' can take place, the focus should rather be on the purpose of the transaction, the intention to make the data accessible to parties in a third country, and the risks associated with it. All of these factors should be given weight when determining whether 'transfer' of data takes place or not. They should not be cumulative, but rather interplay with one another. By doing so, it is possible to provide a technology neutral definition, which may be applied to new forms of technology that may emerge. A definition of the concept should be interpreted broadly, as a narrow definition would most likely not encompass all the emerging ways in which data may be transferred in the future.

Regarding the purpose factor, the main criteria should be whether the purpose of the transaction is to process the data in a third country. This criterion would focus on the need to protect the data where they are processed, which would safeguard the fundamental rights and freedoms of EU citizens. To give an example, this factor would require the purpose of uploading data onto the Internet, to be assessed. If the purpose of doing so is for example that the data be downloaded in a third country in order to be used for consultation purposes, such acts would most likely fall under the definition, unless the other factors strongly weigh against it.

The risks associated with the transfer could serve as a factor that could exempt a transaction that falls under the definition of 'transfer' from the restrictions applicable, and as a factor that increases the likelihood of finding that 'transfer' takes place. For example, the risks associated with the transfer could be mitigated by taking certain technological measures to protect the data, such as through the use of privacy by design. In this sense, the risk factor would be in line with the rationale behind the rules, by ensuring the fundamental rights and freedoms of data subjects with respect to the processing of personal data, through technological means. On the other hand, not taking any such measures could
increase the likelihood of 'transfer' taking place. The role that technology can play in protecting data under transfer has unfortunately not been sufficiently recognised. Even though technology constantly creates new legal problems relating to what constitutes 'transfer', it should increasingly be used to reduce the risks associated with 'transfers' of data.

The factor relating to intention could be used as criteria for determining whether or not the acts in question fall under the definition, or whether a further analysis is required, where the implications of Lindqvist would come into play. In cases where intention exists to make data for example accessible to predefined persons or organisations in third countries, such acts should fall under the definition.

In cases where intention to make the data accessible to parties in third countries is absent, the factors to be read from Lindqvist should be taken into account. This may further be supported by the approaches taken in Germany and by the UK ICO. The main factors to take into account in such cases are the consequences of finding that 'transfer' takes place, and whether the 'direct transfer' requirement is fulfilled. If a finding that 'transfer' takes place makes the restrictions on transfer of general application to the entire Internet, the acts in question should not fall under the definition. If not, the acts should fall under the definition, given that there is proof of a grant of actual access. The applicability of the definition and the restrictions it triggers would thus be limited to some extent.

Under this approach, the intention factor would in any case require there to be a sufficient connection with the third country in question, which would justify assessing the level of protection in that country. Account should further be taken of the purpose of the transfer, and the risks associated with it, independently of whether intention to make the data accessible exists or not.

Under the aforementioned factors, making data intentionally accessible on a large scale and for business purposes would fall under the definition. Instances where a controller uploads
data to servers located in a third country knowingly or intentionally, for the purposes of processing, would also fall under the definition. If a controller uploads data to servers unknowingly or without making inquiries regarding their location, the purpose of the act of uploading should be considered when assessing whether such acts fall under the definition. If the acts are found to fall under the definition, technical measures taken by the controller to protect the data could in all of the aforementioned cases exempt the ‘transfer’ from the restrictions applicable.

In light of this, my suggestion of how the concept of ‘transfer’ of data should be defined is the following:

"Transfer’ of data means the act of transmitting data to a third country for the purposes of processing or making the data intentionally accessible to parties in third countries. If data are accessed without intentionally being made accessible, the consequences of finding that ‘transfer’ takes place must be assessed. Adequate technological measures that protect the data may exempt the transfer from restrictions.

This is only a suggested definition, but gives in my opinion a good guidance of how the concept ‘transfer’ of data to third countries should be defined, preferably in the GDPR. Defining the concept in this way would make this field of law much clearer, effective and adjust it to the realities of modern technology, without being technology-dependent.

Turning to possible limitations of this definition, the main limitation is that some agreement between regulators and governments would need to be reached regarding what kind of technological measures should be sufficient to exempt certain transactions, which fall under the definition, from restrictions. The weight of the factors would also need to be addressed in practice. Even though I am of the opinion that they should interplay with one another, it is challenging to assert exactly how the balance of interest assessment should be
carried out, without knowing which technological measures would be required in order to exempt certain transactions from the restrictions that follow of the definition.

Regarding future implications, it is difficult to tell whether EU legislators will define the concept of 'transfer' of data in the GDPR. I am of the opinion that they should do so, and if not, that they as a minimum should seek to create some legal guidance on the matter. This could for instance be done through providing examples of circumstances where transfer would, or would not, take place. Another solution would be to not require a separate legal basis for transfers of data to third countries. Doing so might solve the whole problem in its entirety, as in such cases it would be sufficient to treat 'transfer' as a form of processing, with all the applicable legal requirements that apply to processing of personal data.

With that being said, I am of the opinion that the rationale behind the rules must always be kept in mind when defining whether restrictions on 'transfer' of data are applicable. If the freedoms and rights of EU citizens are endangered by the transaction in question, it should fall under the definition of 'transfer' of data. The aforementioned factors I’ve provided for the definition are aimed at taking into account this rationale, and should thus be interpreted with that in mind.
7 Table of reference

Books and journal articles


**Reports, opinions and other documents**


Legislation


**Case law of the Court of Justice of the European Union**

Case C-101/01, Bodil Lindqvist [2003] ECR I-12971, judgment of 6 November 2001

Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2015] ECR-00000, judgment of 6 October 2015
Decisions by the Norwegian Privacy Appeals Board

PVN-2013-05, *Diakonhjemmet sykehus*, decision of 13 December 2013

PVN-2013-08, *Haraldsplass Diakonale Sykehus*, decision of 20 December 2013

PVN-2013-09, *Helse Bergen*, decision of 20 December 2013

PVN-2013-11, *Oslo universitetssykehus*, decision of 20 December 2013

PVN-2013-12, *Curato Røntgen*, decision of 20 December 2013

PVN-2014-22, *Vestre Viken HF*, decision of 13 August 2015