The Right to Data Portability in Article 20 of the General Data Protection Regulation

An analysis of the legal obligations for data controllers when data subjects requests the right to data portability.

Candidate number: 9003

Submission deadline: 1.12.2017

Number of words: 17918
# Table of contents

**LIST OF ABBREVIATION** ........................................................................................................ 1

1 **INTRODUCTION** ............................................................................................................. 2

1.1 Research question .............................................................................................................. 3
1.2 Structure ............................................................................................................................ 3
1.3 Methodology ....................................................................................................................... 4
1.4 Demarcation ....................................................................................................................... 6

2 **THE MAIN ELEMENTS OF THE RIGHT TO DATA PORTABILITY** .................. 8

2.1 The right to receive personal data ..................................................................................... 8
   2.1.1 Is the right to data portability merely just an extension of the right of access? ....... 9
2.2 The right to transmit personal data .................................................................................. 9
2.3 Clarifying undefined terms in the right to data portability ............................................ 10
   2.3.1 What constitutes as structured, commonly used and machine-readable format? .... 11
   2.3.2 The criterion of without hindrance .......................................................................... 12
   2.3.3 What constitutes as technically feasible? ................................................................ 13

3 **WHEN DOES THE RIGHT TO DATA PORTABILITY APPLY?** .................. 14

3.1 First condition: Lawful processing ................................................................................... 14
   3.1.1 Data subject’s consent ............................................................................................... 14
   3.1.2 On performance of a contract ................................................................................... 17
3.2 Second condition: Personal data concerning, and provided by, the data subject .......... 18
   3.2.1 The personal data concerning the data subject ....................................................... 18
   3.2.2 Data provided by the data subject .......................................................................... 22
3.3 Third condition: The rights and freedoms of others ....................................................... 25

4 **PORTABLE DATA FROM FITNESS WEARABLES (INTERNET OF THINGS)** ....................................................................................................................... 29

4.1 Do the service providers of fitness wearables let its users import and export data? ...... 30
4.2 Does the right to data portability apply for fitness wearables? .................................... 31
   4.2.1 The Regulation’s extra-territorial applicability ......................................................... 31
   4.2.2 Lawful processing ..................................................................................................... 32
4.3 Are the activities tracked by fitness wristbands personal data “provided by” the data subject? ................................................................................................................. 33
5 GENERAL RULES WHEN ANSWERING DATA PORTABILITY REQUESTS

5.1 The obligation to provide information on the existence of the right to data portability 36
5.2 Identification of the data subject ................................................................. 37
5.3 What is the time limit to answer a data portability request? ......................... 38
5.4 Could a portability request be rejected or a fee charged? ................................ 39
5.5 Securing portable data.................................................................................. 40
5.6 What if data controllers do not comply with their obligation for data portability? .... 42
   5.6.1 What mechanisms may a data subject use? .............................................. 43

6 CONCLUSION....................................................................................................... 44

6.1 Further research............................................................................................ 46

TABLE OF REFERENCE ....................................................................................... 48

Statutes ................................................................................................................. 48
Court decisions ...................................................................................................... 48
Publications from authorities................................................................................. 49
Books .................................................................................................................... 50
Articles in electronic journals................................................................................. 50
Other secondary sources....................................................................................... 52
Web pages ............................................................................................................ 53
List of abbreviation

EEA – European Economic Area
EU – European Union
GDPR – General Data Protection Regulation
IoT – Internet of Things
RtDP – The right to data portability
WP29 – Article 29 Data Protection Working Party
1 Introduction

With rapid technological developments and globalization, the scale of personal data being processed and collected have increased\(^1\), and personal data is termed to be “the new oil”\(^2\). Individuals provides personal data to several service providers, but challenges are being presented when an individual wants to change service provider.

The European Commission have stated that “with increasing use of certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy friendly services become available”\(^3\). A consequence of this could be “loss of contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data which is very difficult to recreate or restore”\(^4\). When an individual is not able to bring with them such personal data, it could create a lock-in effect with the specific service provider, and obviously the individual does not have control over its data.

The General Data Protection Regulation\(^5\) replacing Directive 95/46/EC effective May 25, 2018\(^6\), will be applicable for the Member States in the European Union (EU) and European Economic Agreement (EEA). With this, data privacy law within the EU undergoes changes, and the Regulation will lead to harmonisation of data protection across the EU and within the EEA.

The Regulation is a part of the EU Data Protection Reform, which is intended to make Europe fit for the digital age. The European Commission states the following about the purpose of the reform:

The reform will allow people to regain control of their personal data. Two-thirds of Europeans (67%), according to a recent Eurobarometer survey, stated they are concerned about not having complete control over the information they provide online. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed. The data protection reform will strengthen the right to data

---

\(^1\) Regulation (EU) 2016/679, Recital (6).
\(^2\) Bygrave, Data Privacy Law, 4.
\(^3\) European Commission, Impact Assessment, 28.
\(^5\) In this thesis, GDPR and the Regulation, are used interchangeably to refer to the General Data Protection Regulation (EU) 2016/679.
\(^6\) GDPR, Article 99 (2).
protection, which is a fundamental right in the EU, and allow them to have trust when they give their personal data\(^7\).

The right to data portability\(^8\), among the other data subject rights, will address these concerns by empowering data subjects with more control over their personal data\(^9\).

### 1.1 Research question

The right to data portability will, according to Recital 68 of the Regulation, strengthen data subjects control over their personal data. Thus, what is the legal content of this right? The right to data portability raises several questions, and the following questions will be addressed in this thesis:

1. What are the legal obligations for data controllers\(^10\), and when does the right apply?
2. Which personal data is recognized as “provided by” data subjects? For example, will data controllers be obligated to include activities tracked by fitness wearables?
3. How will the general rules in the Regulation concerning rights of the data subject apply to the right to data portability?

### 1.2 Structure

The thesis is organized into seven chapters, including the introduction chapter. In this chapter I address the thesis methodology and provide demarcations for the research question.

The second chapter address what the main elements of the right to data portability, and whether the RtDP is merely an extension of the right of access. Additionally, I will clarify the undefined terms, the criterions “structured, commonly used and machine-readable format”, “when technically feasibly”, and “without hindrance”\(^11\).

\(^7\) European Commission, Press release, 15 December 2015.  
\(^8\) In this thesis, the right to data portability and the RtDP, are used interchangeably to refer to the right presented in GDPR Article 20.  
\(^10\) GDPR, Article 4 (7) defines a data controller as “natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data [...].”  
\(^11\) GDPR, Article 20 (1).
In the third chapter, I will address when the right to data portability applies. The application of the right will be based on the three cumulative conditions; 1) lawful processing, 2) personal data concerning, and provided by, the data subject, and 3) the rights and freedoms of others.

The fourth chapter address the specter of Internet of Things, where I will use fitness wearables as an example to address what constitutes as personal data “provided by” the data subject. I will discuss whether personal activities tracked by a wearable device constitute as data “provided by” the data subject.

In the fifth chapter, I will address general rules governing data controllers’ obligation to the right to data portability. Additionally, I will briefly address the remedies and penalties for data controllers’ infringements on the right to data portability.

The sixth chapter will present the conclusion on the research question and comments on further research on the topic of data portability.

1.3 Methodology

The General Data Protection Regulation is secondary EU law which have general application and is binding in its entirety and directly applicable in all Member States\textsuperscript{12}. Secondary law is hierarchical below EU treaties and general principle of EU law.

This thesis addresses the right to data portability in a doctrinal legal research to determine its legal scope. I will determine the legal relevance of the sources used in the thesis.

The treaties of the European Union\textsuperscript{13} do not explicitly regulate the interpretation of EU law. However, methods of teleological, analogic, contextual and literal (textual) interpretation are accepted in European Union Law. Additionally, the Court of Justice of the European Union (hereinafter the Court) have clarified interpretation of the languages within Member States in the CILTIF-case\textsuperscript{14}. The Court provides that interpretation of a provision in community law involves a comparison of different language versions, as all versions are equally authentic. Secondly, the Court emphasize that legal concepts may have different meaning in community law and in the law of the Member States, bearing in mind the terminology peculiar to community law. Finally, the Court provides that an interpretation of a provision must be within

\textsuperscript{12} Treaty on the Functioning of the European Union (OJ C 202 (2016)), Article 288 second paragraph.


\textsuperscript{14} Case 283/81. "CILTIF", paragraph 18-20.
its context and in light of the community law as a whole, keeping in mind the objectives and its state of evolution.

The main legal source used in the thesis is the General Data Protection Regulation including its Recital. The Recital will be an important source when interpreting the provisions with the objective of the Regulation.

An important legal source for EU law are court decisions. However, there are no existing court decisions for the GDPR, as the Regulation is not yet applicable.

The first legislative proposal of the GDPR was published in 2012 and the final text was published in 2015. The preparatory works (travaux préparatoires) will demonstrate the intention behind the EU legislation. However, it does not bear any significant weight of interpretation.

The legal doctrinal research on the right to data portability will also rely on secondary sources from authorities and available doctrine in the academic literature.

A unique source in EU data protection law, is opinions, recommendations and guidelines from the Article 29 Data Protection Working Party. The Working Party is an independent advisory body, composed of representatives from supervisory authorities, authorities established for the EU institutions and bodies, and the European Commission. However, these sources do not have binding force, but indicate the consensus on current law among the supervisory authorities.

There will be some degree of uncertainty regarding interpretation of the obligations presented in the right to data portability. The Guidelines from the Working Party and research articles will serve the purpose of indicating the degree of uncertainty, were it may range from consensus to conflicting interpretations of the GDPR. The degree of uncertainty might indicate that a certainty requirement or term are sufficiently clear, and where there is a high degree of uncertainty, or even conflicting interpretation, will make it difficult to establish its scope and meaning.

Many of the research articles were written before the final version of Article 20 of the Regulation was adopted. They still have a significant bearing on the matter, as the Proposal for the GDPR bear many similarities with the final version. The WP29 Guidelines on the right to data portability have also been revised after it was adopted in 2016.

15 The terms WP29 and the Working Party, will be used interchangeably to refer to the Article 29 Data Protection Working Party.
I will also address policy statements and other statements, for example press releases from EU and other statements prior to the final text. I emphasize that the sources vary in both formality and prominence. Thus, these public statements could be perceived as key messages, and address the purpose of the Regulation.

As the Regulation has not yet come into application, the legislative processes of implementing the Regulation in the Member States could also bear relevance. Where relevant, I will include the preparatory works in Norway for implementing the Regulation to Norwegian law. The preparatory works includes the Consultation Document from the Norwegian Ministry of Justice and Public Security and the Consultation Response from the Norwegian Data Protection Authority. I will not include responses from other stakeholders, as the preparatory work in the Member States will not be the focus of the thesis. However, it indicates circumstances where the Member States have the option to provide additional provisions on some special circumstances.

I have taken into account a report made by the Norwegian Consumer Council, to address how some fitness wearables cope with data portability today. It will not be used to determine any legal obligation for the data controllers, but as an example to discuss the right to data portability in the specter of Internet of Things.

1.4 Demarcation

This thesis will exclusively address EU privacy law, primarily focusing on the General Data Protection Regulation and the right to data portability, as it is being presented in Article 20 of the GDPR.

Firstly, I will not address the right to data portability in a competition perspective, nor in a consumer perspective. Data portability in a competition perspective, could have been to compare it with Article 102 of the Treaty on the Functioning of the European Union, which prohibits the abuse of a dominant position. Numerous scholars have compared the RtDP with Article 102, stating that Article 102 could be used to enforce data portability as a concept16. However, the Working Party states that even though data portability may enhance competition, the Regulation regulates personal data, and not competition17. In a consumer perspective, the RtDP could have been compared by me to the proposal for a Digital Content Directive.

16 Diker V. And Ursic, “The right to data portability in the GDPR and EU competition law”, 11 (conclusion). See also e.g. Graef et. al., “Putting the Right to Data Portability into a Competition Law Perspective”; Swire and Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare”.
17 WP29, Guidelines on the right to data portability(a) (hereinafter cited as Guidelines v2), 4.
However, this will not be included, as this directive gives the consumer some control over the digital content provided when a contract is terminated, and does not regulate data portability of personal data.

Secondly, complying with the right to data portability might result in personal data being transferred to a country outside the Member States of EU or the EEA. I will not address this, as these circumstances ought to be addressed by other provisions, such as binding corporate rules\(^\text{18}\) or by the EU-U.S. Privacy Shield\(^\text{19}\), pursuant to Articles 44 through 49 of the Regulation. I will not include this, as it will not be within the objective of the thesis.

Thirdly, I will not address how, and if, data processors have to comply to the right to data portability. Such application is pointed out by the Working Party, providing that if the requested personal data are processed by a data processor, the processor have contractual obligations to assist the controller\(^\text{20}\). Such obligations need to be addressed by the data protection agreement between the processor and the controller in conjunction with Article 28 and Recital 81 of the Regulation. This is not addressed by the provisions of the right to data portability in Article 20, which relates to the obligations of the data controllers, and not data processors. The legal obligations of data controllers are within the objective of this thesis, not the obligations for data processors.

Fourthly, as the objective of the thesis is to address data portability of personal data, I will not address the proposed regulation on the free flow of non-personal data within the EU.

Lastly, the Regulation provides for a possibility to introduce restrictions on the right to data portability pursuant to Article 23\(^\text{21}\) and derogations pursuant to Article 89. In Norway, a derogation is proposed, stating data portability will not apply to the processing of personal data solely for archival purposes in the public interest\(^\text{22}\). This derogation has been criticized by the Norwegian Data Protection Authority\(^\text{23}\). Such Member State specific restrictions and derogations will not be addressed in the thesis, as the thesis objective is to address the right to data portability’s legal obligation for data controllers at regional level for the EU as a whole, and not addressing specific restrictions or derogations made by Member States.

---

\(^\text{18}\) GDPR, Article 47.
\(^\text{19}\) European Commission, Commission implementing decision of 12 July 2016.
\(^\text{20}\) WP29, Guidelines v2, 6.
\(^\text{21}\) Restrictions could be introduced for Articles 12 to 22, 35, as well as Article 5.
\(^\text{22}\) The Norwegian Ministry of Justice and Public Security, “Høringsnotat” (Consultation Document), 129.
\(^\text{23}\) The Norwegian Data Protection Authority, “Høringsuttalese” (Consultation Response), 88.
2 The main elements of the right to data portability

Article 20 of the Regulation defines the right to data portability as:

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided […]\(^\text{24}\)

The right to data portability consist of two\(^{25}\) separate data subject rights. Firstly, there is a right to receive personal data. Secondly, there is a right to transmit personal data to another controller\(^{26}\) and where technically feasible, transferring personal data directly from one controller to another. These rights are separate, meaning that the data subject\(^{27}\) may choose either receive the personal data on his or her own choosing. Or, the individual may choose to transfer to personal data to another controller. The individual may request both, but they are not dependent of each other.

2.1 The right to receive personal data

There has been an increase of online services and storage of data on these services. The data vary from different online services, but some examples are personal photos, contact information, calendar history, and personal messages. The Commission have stated that the increased use of online services with no possibility for portability, creates a lock-in with the specific provider\(^{28}\). Further, they state that portability is a key factor for effective competition, as evidence in market sectors such as the telecom sector\(^{29}\). However, the Regulation regulates personal data and not competition\(^{30}\).

Article 20 (1) states that the data subject “shall have the right to receive the personal data concerning him or her, […] in a structured, commonly used and machine-readable format”. A purpose of the right to receive personal data in the RtDP, is to strengthen the data subjects

\(^{24}\) GDPR, Article 20 (1).

\(^{25}\) Three - if the right to transfer personal data is separated between the right to transfer personal data without hindrance and “transfer directly if technically feasible”, cf. GDPR, Article 20 (1) and (2).

\(^{26}\) Any natural or legal person who determines the purposes and means of data processing, cf. Article 4 (7).

\(^{27}\) In this thesis, the terms “data subject”, “individual”, and “user” will be used interchangeably to refer to a data subject.

\(^{28}\) European Commission, Impact Assessment, 28.

\(^{29}\) Ibid. The reference is to number portability, meaning it is the individual owning the number, and not the telecom provider.

\(^{30}\) WP29, Guidelines v2, 4.
control over their own personal data\textsuperscript{31}. With this right, the data subject will be able to store the personal data on his or her own device for personal purposes and further use. This make associations to the right of access\textsuperscript{32}. The right to data portability is being understood as an extension\textsuperscript{33} or related\textsuperscript{34} to the right of access. Article 15 (1) states that the data subject “shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data […]”. 

2.1.1 Is the right to data portability merely just an extension of the right of access?

While the right of access gives an individual the right to obtain personal data in a commonly used electronic form where the data subject makes the request for access by electronic means\textsuperscript{35}, the right to portability gives an individual the right to receive personal data in a structured, commonly used and machine-readable format\textsuperscript{36}. The right of access is a broad right which purpose is to let the data subject be updated on what and how their personal data is being processed. The information you may receive with the data portability may be narrower, as it is limited to personal data provided by the data subject.

Where the right to data portability distinguish from the right of access is where the data subject exercises the right to transmit their personal data from one controller to another\textsuperscript{37}.

2.2 The right to transmit personal data

A data subject can ask the data controller processing its personal data to transmit the data to another controller “without hindrance”\textsuperscript{38}. Where it is technically feasible, the personal data can also be transmitted directly from one data controller to another\textsuperscript{39}. The right of access and the right to data portability will grant data subject the possibility to store their personal data on their

\textsuperscript{31} GDPR, Recital (68).
\textsuperscript{32} GDPR, Article 15.
\textsuperscript{33} Bapat, “The new right to data portability”. Bapat argues that the the right to data portability should be understood as an extension to the current right of subject access. In the paper, Bapat is addressing the Proposal, where the right to data portability was article 18, and 18 (2) stated that data subject had a right to obtain a copy of their personal data.
\textsuperscript{34} WP29, Guidelines v2, 5.
\textsuperscript{35} GDPR, Article 15 (3) cf. (1).
\textsuperscript{36} Article 20 (1).
\textsuperscript{37} Article 20 (1) and (2).
\textsuperscript{38} Article 20 (1).
\textsuperscript{39} Article 20 (2) cf. (1).
private device. While the right to transmit personal data, will ensure that the personal data of a data subject can be reused. This could prevent lock-in circumstances and it gives the data subjects ownership to their personal data.

Upon request by the data subject, personal data can also be transmitted directly from one data controller to another. However, Article 20 provides a limitation for exercising this right, that it has to be “technically feasible”. Data controllers are encouraged to develop interoperable formats that enable data portability\(^{40}\). Thus, there are no obligation for the data controllers to adopt or maintain processing systems which are technically compatible\(^{41}\). This suggest that there is no obligation for data controllers to have systems that can process data from different origins\(^{42}\). Even though the data controllers are not obligated to have compatible systems, the Regulation prohibit data controllers from establishing barriers to the transmission of personal data\(^{43}\).

The right to data portability does not provide for any limitations for specific service providers. This suggest that the individuals may request transmission and reuse of its personal data among various services, either within the same business sector or in any other sector they are interested in\(^{44}\). Additionally, the controller answering a data portability request under the conditions of Article 20, are not responsible for the data processing by the data subject or the controller who receives the personal data\(^{45}\).

### 2.3 Clarifying undefined terms in the right to data portability

Clarifications on some of the key terms of the right to data portability will indicate a broad or narrow exercise of data portability. The applicability of the RtDP is separated to three cumulative conditions discussed in chapter three.

Terms that needs further clarification are, structured, commonly used and machine-readable format, without hindrance, technically feasible, and data provided by the data subject. The latter shall be addressed in chapter three, as it is a key element in a cumulative condition for the

\(^{40}\) GDPR, Recital (68).
\(^{41}\) Ibid.
\(^{42}\) Graef et. al., “Putting the Right to Data Portability into a Competition Law Perspective”, 2. The authors states that the data processors have an obligation to make their data formats “compatible and ensure that their systems can process data from different origins”. However, this was in the legislative process were the term “interoperable” was used instead of “in a commonly used format”.
\(^{43}\) WP29, Guidelines v2, 5; GDPR, Recital (68).
\(^{44}\) WP29, Guidelines v2, 5.
\(^{45}\) Ibid, 6.
applicability of the right to data portability. The others are understood as practical consequences for the controller’s obligation to comply with the right.

2.3.1 What constitutes as structured, commonly used and machine-readable format?

Article 20 (1) states that data controllers have to provide personal data “in a structured, commonly used and machine-readable format”, without clarifying its substance. In addition, Recital (68) states that the format should be “interoperable”, without clarifying the obligations. However, the term “interoperable” is defined in the EU as:

[…] the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems […]

Data controllers can use a wide range of data types. The Regulation does not create an obligation for the controllers to have technically compatible systems, but controllers are encouraged to develop interoperable formats that will enable data portability.

However, scholars have pointed out that data portability must not be confused with interoperability, which goes further than data portability. In context of social networks, interoperability will enable users to connect with other irrespective of their affiliation, meaning that a Facebook user could post a message directly on someone’s Google+ page. By contrast, the interoperable format within the right to data portability is making it possible for individuals to reuse their data. For example, Facebook users could take their data and open a new account on Google+ based on the information.

The Working Party states in its guidelines that the terms “structured”, “commonly used” and “machine readable” are minimal requirements which will facilitate the interoperability of the

---

47 GDPR, Recital (68).
49 Ibid; Graef, “Mandating portability and interoperability in online social networks”, 509-510.
data format\textsuperscript{51}. As the WP29 refers to in their Guidelines, the EU have previously defined the terms\textsuperscript{52}. A format is \textit{structured} if “software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure”\textsuperscript{53}. The format will be \textit{machine-readable} if there is “data encoded in files”\textsuperscript{54}. This means that a software can extract elements of data enabling service providers to use the data.

There is also a requirement of a “commonly used” format. The wording “commonly used” implies that this will differ across business sectors. In the Proposal, the Commission had authority to define what formats meets the requirements. However, in the Regulation it seems to be up to the service providers across the different sectors to agree upon what is “commonly used” format. WP29 states where there is no commonly used format, the controller should provide the personal data in open formats, such as XML, JSON, CSV\textsuperscript{55}.

2.3.2 The criterion of without hindrance

Article 20 (1) provides that the data subjects can transfer their data to another controller “without hindrance” from the controller to which the personal data have been provided. The Regulation does not clarify the scope of \textit{without hindrance}. The wording “without hindrance” implies that the first party could not place any obstacles which will hinder the data subject’s possibility to transfer the data to another controller, or obstacles hindering another controller.

The Working Party affirms that hindrance could be “any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller”\textsuperscript{56}.

Swire and Lagos differentiate between a broad and narrow interpretation of the criterion \textit{without hindrance}\textsuperscript{57}. Under a broad interpretation, they argue that the RtDP requires the service providers to develop an “export-import module” (EIM). This is being understood as software

\textsuperscript{51} WP29, Guidelines v2, 17.
\textsuperscript{52} Ibid.
\textsuperscript{53} Directive 2013/37/EU, Recital 21.
\textsuperscript{54} Ibid.
\textsuperscript{55} WP29, Guidelines v2, 18.
\textsuperscript{56} Ibid, 15.
\textsuperscript{57} Swire and Lagos, “Why the Right to Data Portability Likely Reduce Consumer Welfare”, 344-345. They address the Proposal of the GDPR. However, the criterion of “without hindrance” in the Proposal is withheld in the Regulation. I emphasize that where they state that the language appears to require an affirmative obligation on the first party, should not be used for the same context here, as the language of the article have been changed. I will then not use this as a supportive argument, based on that it could mean that I use their argument beyond what they actually meant.
codes and services which can export data from one controller and import the same data to another controller. Under a narrower interpretation, they state that the criterion will seek to prevent the data controller possessing the data to technically block the transfer of data to another controller\textsuperscript{58}.

The discussion on interoperable format is relevant, as it could act as a hindrance\textsuperscript{59} or enable a seamlessly transfer of data between data controllers\textsuperscript{60}.

2.3.3 What constitutes as technically feasible?

Within the scope of the right to data portability, data subjects can, according to Article 20 (2), have the data directly transferred from one controller to another, “where technically feasible”. The Regulation does not clarify what constitutes as \textit{technically feasible}. The wording indicate that it must be addressed on a case-by-case basis and provides for a dynamic interpretation on the technically capabilities at the time. This is limited, as the Regulation does not create an obligation on controllers to either adopt or maintain compatible processing systems\textsuperscript{61}. A direct transfer could therefore only occur where the communication between the controllers are possible\textsuperscript{62}.

The effective exercise of the right to data portability seems to be up to the service providers, and how they cooperate on the development of interoperable format. The uncertainty on the interpretation of the requirement on \textit{interoperable format} and \textit{commonly used format} shows the need for further clarification on the matter before a practice could be established. This can be achieved by cooperation between the stakeholders by different industry sectors. The Working Party strongly encourages such a cooperation, stating that the stakeholders should cooperate to establish a common set of interoperable formats\textsuperscript{63}.

\textsuperscript{58} Ibid.
\textsuperscript{59} WP29, Guidelines v2, 15.
\textsuperscript{60} Swire and Lagos, “Why the Right to Data Portability Likely Reduce Consumer Welfare”, 344.
\textsuperscript{61} GDPR, Recital (68)
\textsuperscript{62} WP29, Guidelines v2, 16.
\textsuperscript{63} Ibid, 18.
3 When does the right to data portability apply?

The right to data portability applies under three cumulative conditions. Firstly, the requested personal data must be processed by automated means based on the data subject’s consent or on the performance of a contract. Secondly, the requested personal data must concern the data subjects and be provided by them. Thirdly, the requested personal data shall not adversely affect the rights and freedoms of others.

3.1 First condition: Lawful processing

The requested personal data must be processed by automated means based on the data subject’s consent or on the performance of a contract. This excludes the controllers’ obligation to answer a data portability request under all other legal grounds for processing personal data. Additionally, Article 20 (3) and Recital 68 further explicitly exclude data portability in circumstances where the processing is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”. This entails that the RtDP does not apply when the processing is necessary for the controller’s compliance with a legal obligation. For example, a financial institution who process personal data as part of their obligation to prevent and/or detect money laundering and other financial crimes, does not have an obligation to answer a data portability request for those processing operations.

Further, in relation to the first condition, the term “automated means” entails that most paper files are not covered by the right and therefore any human intervention ought to be excluded. Processing is recognized as any “operation or set of operations” on personal data.

3.1.1 Data subject’s consent

Article 20 (1) (a) of the Regulation recognizes two separate circumstances for lawful processing based on “consent”. The data subject’s consent is separated between processing of non-sensitive

---

64 GDPR, Article 20 (1) (a) and (b).
65 Article 20 (1).
66 Article 20 (3).
67 Article 20 (1) (a) and (b).
68 Article 6(1) (c)-(f) cf. Article 20 (1). See also Article 20 (3) and Recital 68, which provides that the right to data portability “should not apply where processing is based on a legal ground other than consent or contract.”
69 This example was also pointed out in WP29, Guidelines v2, 8.
70 WP29, Guidelines v2, 9.
71 GDPR, Article 4(2).
personal data and sensitive personal data\textsuperscript{72}. Non-sensitive personal data are covered by Article 6 (1) (a), while sensitive personal data are covered by Article 9 (2). Additionally, special limitations are provided by Article 8 (1), where there is processing of personal data concerning children.

3.1.1.1 Processing of non-sensitive personal data

Lawful processing of personal data based on “consent” is regulated by Article 6 (1) (a). Article 4 (11) defines consent of the data subject as:

[…] any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her […]

The conditions for consent, cf. Article 7 and Recital (32), (42) and (43), provides for further clarification. When determining whether consent is “freely given”, account should be taken of whether there is imbalance between the data subject and controller, and whether the individual is allowed separate consent to different processing operations\textsuperscript{73}. Where the data subject has “no genuine or free choice” or is “unable to refuse or withdraw consent without detriment” the consent is not regarded as freely given\textsuperscript{74}. Examples of circumstances where there may be imbalance are relationships between employees and employers, and where public authorities are the data controller. Where there is imbalance or the data subject are not allowed separate consent to a specific processing operation, consent will not provide a valid legal ground for the processing of personal data\textsuperscript{75}.

For achieving an “informed” consent, the Regulation provides minimum requirements. The controller must provide its identity and the purpose of the processing of personal data, to the data subject\textsuperscript{76}.

As for the “unambiguous indication”, the Recital requires that the consent must be given by the data subject in a “clear affirmative act”, either by a written (including electronic) or oral

\textsuperscript{72} Sensitive personal data is also understood as special categories of personal data.

\textsuperscript{73} GDPR, Recital (43).

\textsuperscript{74} Recital (42).

\textsuperscript{75} Recital (43).

\textsuperscript{76} Recital (42).
The declaration of consent must be in an “intelligible and easily accessible form” with “clear and plain language” without “unfair terms”. Any infringement of this will not be binding upon the data subject. The Recital states that the affirmative act could be ticking a box on an internet website, but silence, pre-ticked boxes or inactivity will not constitute consent. It is the controller processing personal data based on consent, that has to be able to demonstrate whether the data subject has given its consent.

In addition, data subjects have the right to revoke their consent at any time. As Article 7 (3) states, it should be as “easy to withdraw [consent] as to give consent”. For example, data subjects consenting with ticking a box, should be able to “untick” this box at any time.

 Lastly, when assessing whether a consent is freely given, Article 7 (4) states that, utmost account “shall be taken of whether, inter alia, the performance of a contract, including the provisions of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract”.

3.1.1.2 Processing of personal data concerning children

Many service providers have age limits for their users. For example, the social networks Facebook and Google requires that their users are at least 13 years old. Facebook has 2,01 billion active users per month. The fact that 4 percent of the female users and 5 percent of the male users on Facebook are in the age group 13 to 17 years old, indicates that a large proportion of minors use social networks.

The Regulation provides an age requirement of 16 years in order to provide a valid consent for processing of personal data. However, Member States may provide by law a lower age requirement for a child’s consent, thus not below the age of 13. The Norwegian Ministry of Justice and Public Security advise that the age limit in Norway for a child’s consent (without

77 Recital (32).
78 Which is pre-formulated by the data controller, cf. Recital (42).
79 GDPR, Article 7 (2) and Recital (42).
80 Article 7 (2).
81 Recital (32).
82 Article 7 (1) and Recital (42).
83 Facebook, “How do I report a child under the age of 13?”; Google, “Age requirements on Google Accounts”.
84 Facebook, “Facebook Reports Second Quarter 2017 Results”.
85 Statista, “Distribution of Facebook users worldwide as of January 2017, by age and gender”.
86 According to the GDPR, Article 8 (1), processing of personal data of a child below the age of 13 is prohibited.
the parental holder’s consent) should be the age of 13 for Information Society services\textsuperscript{87}, which includes social networks.

Where the child is below the age of 16 years, or below the age requirement provided by law of the Member State, the data controller must ensure that the consent is “given or authorized” by the holder of parental responsibility over the child\textsuperscript{88}.

The data controller is required to make “reasonable efforts” in verifying whether the consent is given or authorized by the parental holder. The Regulation does not clarify what constitutes as “reasonable efforts”, other than taking into account the “available technology”\textsuperscript{89}. A solution can be that the service providers facilitate the use of electronic credentials for secure identification online. Another solution is for example, when the parental holder already has an account on a social network, they could use that account to give or authorize the consent of the child.

3.1.1.3 Processing of sensitive personal data

Processing sensitive data is in general prohibited, cf. Article 9 (1). However, this prohibition may be lifted in some circumstances\textsuperscript{90}. One example where the prohibition could be lifted is where the data subject has given “explicit consent” to the processing of the sensitive personal data\textsuperscript{91}. This means where the individual has not explicitly consented to the processing of its sensitive data, the controller cannot rely on the individuals consent as a legal ground for processing sensitive personal data. Thus, the Regulation states that there may be circumstances where Union or Member States law does not let the data subjects lift the prohibition on processing of sensitive data\textsuperscript{92}.

Where the processing of sensitive data is lawful with data subjects explicit consent, the sensitive data will be within the scope of the right to data portability\textsuperscript{93}.

3.1.2 On performance of a contract

\textsuperscript{87} The Norwegian Ministry of Justice and Public Security, “Høringsnotat” (Consultation Document), 115.
\textsuperscript{88} GDPR, Article 8 (1).
\textsuperscript{89} Article 8 (2).
\textsuperscript{90} Article 9 (2) (a)-(j).
\textsuperscript{91} Article 9 (2) (a)
\textsuperscript{92} Ibid.
\textsuperscript{93} Article 20 (1) (a).
Another alternative for lawful processing where the right to data portability applies, is where the processing is “necessary” for the “performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract”\textsuperscript{94}.

The assessment of what constitutes as \textit{necessary} have to be addressed on a case-specific basis. The Recital (44) provides that the processing is only lawful where it is “necessary in the context of a contract” or necessary for the “intention to enter into a contract”.

The rules on processing personal data concerning children as presented in Article 8 (1) are limited to what is required by the general contract law of Member States\textsuperscript{95}. Contract law of a Member State concerning the “validity, formation or effect of a contract in relation to a child” will not be affected by the requirements presented in Article 8 (1).

3.2 Second condition: Personal data concerning, and provided by, the data subject

3.2.1 The personal data concerning the data subject

Personal data was, in the Proposal, defined as “any information relating to a data subject”\textsuperscript{96}. This definition was amended and specified by the European Parliament and further included in the final text of the Regulation. The Regulation defines personal data as:

\[\ldots\] any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person\textsuperscript{97}.

Defining which personal data is covered by the right to data portability, is vital to understand the right’s scope when an individual request the right. For instance, it is clear that anonymous data or personal data which does not concern the data subject, will not be within the scope\textsuperscript{98}. Therefore, it seems that a necessary assessment in evaluating what types of data that are

\textsuperscript{94} Article 6(1)(b).

\textsuperscript{95} Article 8(3).

\textsuperscript{96} Proposal for a General Data Protection Regulation, Article 4 (1).

\textsuperscript{97} GDPR, Article 4 (1).

\textsuperscript{98} Recital (26); WP29, Guidelines v2, 9.
covered, will be to determine whether the data could identify, or be able to identify, a natural person.

When determining whether a natural person is identifiable or not, Recital (26) provides a proportionality test. In the determination, identifiability is relative to “the means reasonably likely to be used” (such as singling out), taking into account “all objective factors”. Recital (26) provides for objective factors such as available technology at the time, costs and the amount of time required, to identify a natural person. The Regulation does not clarify how extensive the requirements are. These objective factors indicate that where it is costly and requires severe amount of time, the data will not be recognized as identifiable to a natural person.

Some further clarification can be found in the Breyer case, where the EU Court of Justice addressed the definition of personal data under the Directive 95/46/EC. The Court ruled that it is not required that the information necessary to identify a data subject is held by one person.

Additionally, in relation to the determination of means reasonably likely to be used that it will not be the case where “the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant”.

3.2.1.1 What about personal data which undergoes “pseudonymisation”?

Related to the determination of whether a natural person is identifiable or not, are circumstances where the personal data undergoes pseudonymisation. “Pseudonymisation” is defined in Article 4 (5) as:

[…] the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person […]

This should not be understood as making the data anonymous, as additional information could be attributed to a natural person, and then used to identify the data subject. If additional

---

99 GDPR, Article 20 (1) cf. 4 (1).
100 Case C-882/14.
101 Ibid, paragraph 42.
102 Ibid, paragraphs 45 and 46.
103 GDPR, Recital (26).
information could not be attributed to a natural person, that information will not be within the scope. The Working Party states that pseudonymous data are within the scope, as the data clearly can be linked to a data subject where the individual provide respective identifies. This means when the controller is not able to identify the data subject, the individual could provide additional information which will enable his or her identification.

3.2.1.2 Will personal data concerning several individuals be included?

In many circumstances, data controllers process information that contains the personal data concerning multiple data subjects, for example a photo on social networks, or interpersonal messaging on services. A relevant question is whether personal data concerning several individuals will be regarded as “personal data concerning” the data subject who makes the portability request. The uncertainty are whether “concerning” only applies to a natural person where the personal data only concerns him or her, or whether “concerning” applies to a natural person in all cases where personal data concerns him or her.

A restrictive or narrow interpretation of this requirement will prevent achieving the purpose of this right, to empower data subjects control over their own personal data. Social networks, among other service providers, will in some circumstances process personal data concerning numerous individuals in the same data. A restrictive interpretation of the requirement could mean that data subjects will not be able to bring personal data such as photos, contacts, interpersonal messages, to another service provider. However, in a broader interpretation of the requirement, “concerning” may imply that as long as the individual is identifiable in the personal data is sufficient, this could be included in the portability. A broad interpretation seems therefore to be most appropriate. The right is in any circumstances limited to the third cumulative requirement, where it affects “the rights and freedoms of other”.

The Working Party states that data controller “should not take an overly restrictive interpretation of the sentence ‘personal data concerning the data subject’”. WP29 also states that “subscribers should be able to have these records provided to them in response to data portability requests, because the records are [also] concerning the data subject”. The Working

104 WP29, Guidelines v2, 9.
105 GDPR, article 11 (2).
106 Article 20 (1).
107 Recital (68).
108 Article 20 (4).
109 WP29, Guidelines v2, 9.
110 Ibid
Party states further that “where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties”\textsuperscript{111}. The Working Party argues for a broad interpretation of “concerning” and provides that the limitation of the interpretation will be where it “adversely affect the rights and freedoms” of the other individuals identified in the personal data.

3.2.1.3 Special categories of data

Personal data can be categorized in two forms of data. This is the distinction between non-sensitive and sensitive (special categories of) personal data. This is originally a distinction presented in the Directive 95/46/EC, which is upheld in the Regulation. The distinction of these categories is being made of what they “reveal” about an individual\textsuperscript{112}.

Special categories of personal data are recognized as personal data revealing “racial\textsuperscript{113} or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, […] genetic data\textsuperscript{114}, biometric data\textsuperscript{115}, data concerning health\textsuperscript{116} [and] data concerning a natural person’s sex life or sexual orientation”\textsuperscript{117}.

Data concerning health includes all data pertaining to the “health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject”\textsuperscript{118}.

Photographs concerning one or more individuals, should not systematically be considered as sensitive data, because they are only recognized as biometric data when processed through a

\textsuperscript{111} Ibid.
\textsuperscript{112} GDPR, Article 9 (1).
\textsuperscript{113} Whereas GDPR, Recital (51), clearly states that the term “racial origin” do not imply that the European Union accept the existence of separate human races. Thus, what’s recognized as “racial origin” will regardless be recognized as sensitive data.
\textsuperscript{114} Article 4 (13) defines “genetic data” as “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”.
\textsuperscript{115} Article 4 (14) defines “biometric data” as “personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”.
\textsuperscript{116} Article 4 (15) defines “data concerning health” as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”.
\textsuperscript{117} Article, 9 (1).
\textsuperscript{118} Recital (35).
“specific technical means allowing the unique identification or authentication of a natural person”\(^\text{119}\).

De Hert and Papakonstantinou, states that “common data [non-sensitive data] may be used to reveal sensitive information”\(^\text{120}\). For instance, surnames, meal preferences, relationship status on social networks, and purchase behavior of products\(^\text{121}\), may reveal religion, race, sexual orientation, and health. The activities logged on health apps and/or fitness wearable may also indicate the health status of the individual. De Hert and Papakonstantinou argue, even though the verb *revealing* “could denote a dynamic interpretation that could be adapted to processing circumstances, this had not proved to be the case in the past”\(^\text{122}\). Further, they describe the distinguishing factor between non-sensitive and sensitive personal data is based on “its nature and not its potential uses”. It is uncertain whether non-sensitive data revealing sensitive data will be categorized as sensitive under the Regulation.

### 3.2.2 Data provided by the data subject

Defining what data is covered by the right to data portability is vital to understand how data controller must comply with portability requests. The literature and comments related to the Proposal of the Regulation showed great uncertainty of what data is covered by the right. Article 18 (2) of the Proposal for the GDPR included “other information provided by the data subject”, as well as personal data provided by the data subject. However, “other information” are not included in the final text of the Regulation, and some uncertainty about the right has been excised. According to Swire and Lagos, uncertainty was presented that it was a complex task to determine what information was “provided by the data subject”\(^\text{123}\). They argue that directly uploaded data, where the user itself supplies the information, would presumably fall within the definition of “other information”. While data created by a website, such as metadata and aggregated usage data for analysis purposes, presumably are not within the definition of “other information provided by the data subject”\(^\text{124}\). The uncertainty was between these two ends, where they stated that there was no natural line of demarcation.

Even though this uncertainty is not relevant to the Regulation, there are uncertainty of the natural line of demarcation of what is constituted as personal data “provided by” the data

---

\(^{119}\) Recital (51).

\(^{120}\) de Hert and Papakonstantinou, “The proposed data protection Regulation replacing Directive 95/46/EC”, 183.

\(^{121}\) For example, the company Target analyzed patterns of products to identify customers who were pregnant. Daily Mail, “How Target knows when its shoppers are pregnant”.


\(^{124}\) Ibid.
subject. Most of the data on the internet are generated by a combination of the users and the service providers activity.

The condition of provided by the data subject will narrow the personal data which may be included in data portability right. The data set of a data subject will vary a lot depending on the service. There will be variations on the amount of personal data the data subject actively provides to the controller and the amount of personal data the controller or the service provider generates.

The Regulation does not clarify what the term “provided by” means. There are some different opinions on how “provided by” should be interpreted. The Working Party argues for a broad interpretation\(^{125}\), while others argue that this broad interpretation is beyond what the legislators meant\(^ {126}\). A literal interpretation of the wording “provided by” indicate that a data subject in some circumstance can provide data to a controller both actively and passively.

The Working Party states that following categories can be qualified as provided by the data subject: “Data actively and knowingly provided by the data subject [and] observed data provided by the data subject by virtue of the use of the service or the device”\(^ {127}\). The latter, could also be understood as data passively provided by the data subject.

### 3.2.2.1 Data actively and knowingly provided by the data subject

The Working Party gives examples of what kind of personal data they include in this context, as “mailing address, user name, age, etc.”\(^ {128}\). These data will for example be submitted in online forms. Additional personal data may be common, depending on the online form and what is required by the service provider, such as, name, location, date of birth and so forth. In reference to the wording “etc.” from the WP29, the list is not extensive. It seems reasonable to assume that all personal data submitted in online forms will be “data actively and knowingly provided by the data subject”. The individual is actively giving the personal data to the controller and knows which personal data it has given to the data controller.

According to Graef et al.\(^ {129}\), prior to the Guidelines, personal data such as profile information, which a data subject has inserted into a social network will probably fall within the scope, while...

---

\(^{125}\) WP29, Guidelines v2, 10.

\(^{126}\) IAPP, “European Commission, experts uneasy over WP29 data portability interpretation”.

\(^{127}\) WP29, Guidelines v2, 10.

\(^{128}\) Ibid, 9.

\(^{129}\) Graef et. al., “Putting the Right to Data Portability into a Competition Law Perspective”, 4.
statistics for analytical purposes will most likely fall outside the scope. They expressed that the Proposal does not clarify the status between these two scenarios. Further, stating that the right to data portability will enable social media users the possibility to transfer their profile, contacts, photos and videos from a social media site to another. When this was written, it was based on the Proposal’s Recital where social networks were listed as an example\textsuperscript{130}. Profile information, are probably within the scope, similar to “data actively and knowingly provided by the data subject” presented in the Guidelines\textsuperscript{131}. This is data which commonly will be submitted in online forms.

In the context of a line of demarcation, Graef et al., argues that statistics for analytical purposes, probably will fall outside the scope of the right\textsuperscript{132}. This links the relevance for the second circumstance presented by the Working Party, stating that “observed data” are within the scope of the right, limited to data created by the controller\textsuperscript{133}.

3.2.2.2  Observed data provided by the data subject by virtue of the use of the service or the device

When individuals use services, data controllers may have the ability to store different types of data activities of individuals. As discussed in the subsection of personal data concerning data subjects, these data will often be considered as personal data concerning the data subjects. The question in relation to the right to data portability, is whether these personal data are considered to be “provided by” the data subjects. According to the Working Party, the answer will in many cases be; yes. They argue that “provided by” also includes “observed data provided by the data subject by virtue of the use of the service or the device”\textsuperscript{134}. This is to give “full value” to the right.

Observed data was one of the most controversial elements\textsuperscript{135} in the Working Party’s Guidelines on the right to data portability, published in December 2016. This was upheld in the revised and final version of the Guidelines. Observed data will be all observations made on a data set concerning an individual.

\textsuperscript{130} The Proposal for GDPR, Recital 55.
\textsuperscript{131} WP29, Guidelines v2, 10.
\textsuperscript{132} Graef et al., “Putting the Right to Data Portability into a Competition Law Perspective”, 4.
\textsuperscript{133} WP29, Guidelines v2, 10.
\textsuperscript{134} Ibid, 10 and 11.
\textsuperscript{135} IAPP, “European Commission, experts uneasy over WP29 data portability interpretation”.

24
The Working Party provides examples that are within the scope, such as “a person’s search history, traffic data and location data [and] other raw data such as the heartbeat tracked by a wearable device”\textsuperscript{136}. However, they draw the line to were data is created by the data controller using the data observed or directly provided by the individual, for example “a user profile created by analysis of the raw smart metering data collected”\textsuperscript{137}.

Data controllers may have created inferred data and derived data. This data will be created on the basis of the data “provided by” the data subjects. This includes the outcome of an assessment on the health of an individual and profiles created for risk management and financial regulations\textsuperscript{138}. The Working Party argues for a broad interpretation of “provided by” due to the policy objectives of the RtDP\textsuperscript{139}. However, they present a line of demarcation stating that as derived and inferred data are not considered to be “provided by” the data subjects, these data should be excluded from the exercise of data portability\textsuperscript{140}. This means that “provided by” includes personal data related to the activities or results from data subjects’ behavior, but not the data which are a result from analysis of that behavior.

Further, the Working Party states that even though data controllers can exclude inferred data, they should include “all other personal data provided by the data subject through technical means provided by the controller”\textsuperscript{141}. Graef et al., argues that the Working Party seems to balance the RtDP with intellectual property rights with the exclusion of inferred and derived data\textsuperscript{142}.

It seems appropriated to ask whether including observed data will be too great of a liability for data controllers, or whether it is reasonable taking into account the data subjects control over their own personal data. For instance, data portability will not just be relevant for online providers, but all processing of personal data on the basis of the applicability of the right. This includes the specter of internet of things. For instance, fitness wearables track activities, which is presumably important for individuals, and could result in a lock-in effect. This will be discussed in chapter four.

### 3.3 Third condition: The rights and freedoms of others

\textsuperscript{136} WP29, Guidelines v2, 10 and 11.
\textsuperscript{137} Ibid, 10.
\textsuperscript{138} Ibid.
\textsuperscript{139} Ibid.
\textsuperscript{140} Ibid.
\textsuperscript{141} Ibid.
\textsuperscript{142} Graef et al., “Data Portability and Data Control”, 9.
Article 20 (4) of the Regulation states that “the right [to data portability] shall not adversely affect the rights and freedoms of others”. The Recital (68) recognizes circumstances where certain set of personal data could concern more than one data subject, for example pictures and interpersonal messages, and that the right is “without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation”.

According to the Working Party, this condition is intended to avoid cases where the personal data are “likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects”. The third party will most likely in all cases be non-consenting to the processing. The Working Party states that such an adverse effect would occur if the transmission of personal data “would prevent third parties from exercising their rights as data subjects” under the Regulation.

When a data subject initiate transmission of his or her personal data to another data controller, the data subject will give consent to the new controller, or he or she will enter into a contract with the controller. The transfer of personal data concerning more than one subject will include non-consenting data subjects. The new data controller must identify another legal basis for processing of such personal data. The Working Party provides for an example, “a legitimate interest may be pursued by the data controller under Article 6(1)(f), in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for ‘purely personal or household activity’.”

The rights and freedoms of third parties will “not be respected if the new data controller uses the personal data for other purposes, for example if the receiving data controller uses personal data of other individuals within the data subject’s contact directory for marketing purposes”. This is also provided by the principle of purpose limitation, stating that the personal data cannot be processed in a manner that is “incompatible” with the purposes.

To prevent adverse effects on third parties, “the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the

---

143 WP29, Guidelines v2, 11.
144 Such as the data subject rights pursuant to Articles 12 to 23 of the Regulation.
145 WP29, Guidelines v2, 11.
146 Ibid.
147 Ibid.
148 Ibid, 11 and 12.
149 GDPR, Article 5 (1) (b).
requesting user and is only managed for purely personal or household needs\textsuperscript{150}. Therefore, the receiving data controller cannot use the transmitted personal data concerning third parties for its own choosing\textsuperscript{151}.

In addition, there could be circumstances where the requested data set could affect trade secrets and intellectual property. Article 20 (4) does not address trade secrets and intellectual property, per se. However, restrictions on the right to data portability where the portability may affect trade secrets and intellectual property rights have been stated in the literature.

In the “trialogues” of the Regulation, the General Approach of the Council stated that “the right referred to in paragraph 2 [the right to data portability] shall not apply if disclosing personal data would infringe intellectual property rights in relation to the professing of those personal data”. This was not included in the final text of the Regulation.

Diker V. and Unver stated, prior to the publication of the Guidelines, that there was a need for further clarification whether the right would be restricted if affecting “proprietary information and intellectual property rights”\textsuperscript{152}. They conclude it should be the case, as the right is understood as an extension of the right of access, which could be restricted if it “adversely affects the rights and freedoms of others, including trade secrets and intellectual property rights”\textsuperscript{153}. If that is the case, similar to the rights and freedoms of others, data controllers would be able to remove data before complying with portability requests. Nevertheless, Diker V. and Unver recognize that neither the Recital 68, nor Article 20, of the Regulation address trade secrets and intellectual property\textsuperscript{154}.

The Working Party states, at the same time clarifying that it is not directly related, that the rights and freedoms of others can be “understood as including ‘trade secrets or intellectual property and in particular the copyright protection the software’”\textsuperscript{155}. In the absence of a clear link between data portability and intellectual property, WP29 lean on Recital 63 of the Regulation which address limitations on the right of subject access. When stating that this should be considered before the data controller answer a data portability request, WP29 refer to Recital 63 of the

\textsuperscript{150} WP29, Guidelines v2, 12.
\textsuperscript{151} Ibid.
\textsuperscript{152} Diker V. And Unver, “The right to data portability in the GDPR and EU competition law”, 4.; This was also problematized in Swire and Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare”, 348. They stated that article 18 of the Proposal, failed to address the right to data portability in connection with intellectual property rights.
\textsuperscript{153} GDPR, Recital (63).
\textsuperscript{154} Diker V. And Unver, “The right to data portability in the GDPR and EU competition law”, 4.
\textsuperscript{155} WP29, Guidelines v2, 12.
Regulation, with the provision that “the result of those considerations should not be a refusal to provide all information to the data subject”\textsuperscript{156}.

It poses uncertainty whether and how restrictions of data portability would be addressed in circumstances where it may affect trade secrets and intellectual property of data controllers. The legal basis, as presented in the literature, for restrictions, is Recital 63 which addresses the right of subject access. Since, the right to data portability has a connection to the right of access, it seems plausible that this may be a correct interpretation. Article 20 (4) itself, does not address trade secrets and intellectual property. However, a literal interpretation of the wording “others” indicate that both natural persons and legal persons should be taken into account, when considering the rights and freedoms of others.

\textsuperscript{156} Ibid.
4 Portable data from fitness wearables (Internet of things)

The internet of things (IoT) have had enormous growth the last decade. The analyst firm Gartner forecasts that there will be 8.4 billion connected things in use worldwide in 2017, and that it will reach 20.4 billion by 2020\textsuperscript{157}. Most of these devices are being used by consumers. The Working Party refers to the following on the concept of IoT:

An infrastructure in which billions of sensors embedded in common, everyday devices – “things” as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using network capabilities […]\textsuperscript{158}

Simplified, IoT is a term for devices that connects over the internet. Today, Internet of Things is everywhere in our daily life. There is wearable computing which can record and transfer data, and quantified self-things which can record information about the user’s habits and lifestyle. There are also domotics at home or the office, where devices such as light bulbs, alarms, weather stations, oven, and kettle, can be connected and controlled over the internet. The Working Party emphasize that these three categories of devices are exemplary of most of the IoT available today\textsuperscript{159}. A device can be linked to more than one category, depending on the devices\textsuperscript{160}. Presumably, no one could have anticipated this development of devices back in mid 1990, when the pre-Internet Directive 95/46/EC was enforced. The Internet of Things has presented great innovations, but also great concerns for data privacy. The Working Party also recognize this providing that the development of IoT “clearly raises new and significant personal data protection and privacy challenges”\textsuperscript{161}. A well-known recent example is the children toys My Friend Cayla and i-Que, which had lack of security, where anyone could take control over the toy with a mobile phone, making it possible to talk and listen through the toy\textsuperscript{162}.

There is especially one category of IoT devices that is popular with individuals, fitness wearables\textsuperscript{163}. Fitness wearables are worn on the body and are classified as wearable computing, but have capabilities of Quantified Self-assessment, meaning that the device have the capability

\textsuperscript{157} Gartner, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent from 2016”.
\textsuperscript{158} WP29, Recent Developments on the Internet of Things, 6. I emphasize that this is an opinion, provided by the WP29 to “contribute to the identification and the monitoring of risks derived from those activities, where the fundamental rights of citizens of the EU are at stake”, 4. Additionally, the opinion is prior to the Regulation. However, their findings are still relevant.
\textsuperscript{159} WP29, Recent Developments on the Internet of Things, 6.
\textsuperscript{160} Ibid.
\textsuperscript{161} Ibid.
\textsuperscript{162} The Norwegian Consumer Council, “Connected toys violate European consumer law”.
\textsuperscript{163} Also known as fitness trackers and fitness wristbands.
to track personal data and assess those data to provide information about the health and wellbeing of the individual. An individual can provide height, weight, gender and age, making the device able to calculate calories burned when exercising. Additionally, the device can track geo location, sleep quality and heart rate, among more, depending on the specific device used. The fitness wearables may have different purposes for the users. Users can use the statistics generated from the exercise for motivation. Users may set yearly goals and use the statistics to analyze how they are doing achieving the goal, and maybe use the previous year’s statistics for cross-referencing. If the individual cannot bring these statistics to another service provider, that might result in a “lock-in” effect. Therefore, it could be important for the users to be able to reuse the data tracked by these devices. An unclear question is whether the data tracked by such devices will constitute as data “provided by” the data subject pursuant to Article 20 (1).

4.1 Do the service providers of fitness wearables let its users import and export data?

The Norwegian Consumer Council published the report *Consumer protection in fitness wearables* in November 2016. They analyzed the four most popular brands on the Norwegian market (Fitbit, Garmin, Mio and Jawbone), based on criterions from the Directive 95/46/EC, among other sources. They also addressed how these devices complied with data portability. The Consumer Council concluded that the service providers had their strengths and weakness, and none satisfied the criteria set by the Council. In relation to portability, their criterion was additional rooted in the right to data portability in the Regulation. Their findings were that Fitbit, Garmin, and Jawbone let the data subjects download their exercise data easily through their websites. Presumably, in .csv and .xls for Fitbit and Jawbone, and another format for Garmin, when the Council wrote the report. Additionally, Mio was in the process of implementing a similar function.

The Council found that only one of the provider let the data subjects upload their data – but not in a file-format used by the other services, such as .csv and .xls. There seems to be few changes to the Council’s findings. I will have a further look at Fitbit and Garmin.

Fitbit lets the user export his or her data in .csv or .xls. The data available for export is body (e.g. weight, bmi and heart rate), foods (any logged foods), activities (e.g. steps taken, total calories burned and distance), and sleep (sleep data). Additionally, GPS data can be exported

---

166 Fitbit, “Can I export my fitness data to my computer?”
Garmin Connect lets the user export their activity data in the formats .tcx, .gpx, or .kml. While through the user profile on the Garmin connect website, there seems to be an option for the users to export all activities in .csv.

Garmin Connect lets users import Garmin Activity Files (.tcx, .fit or .gpx format) and Fitbit body or activity data (.xls, .xlsx or .csv format). A user importing his data from Fitbit to Garmin showed that Garmin Connect analyzed the activities in a different manner, and even some of the data didn’t even show up in Garmin Connect. Fitbit doesn’t seem to let its user import data from another service provider.

4.2 Does the right to data portability apply for fitness wearables?

Due to the scope of the thesis, there will be a brief and general approach to the Regulation’s, and the right to data portability applicability for fitness wearables. The main question is whether the activities tracked by the fitness wristbands could be included in a data portability request.

4.2.1 The Regulation’s extra-territorial applicability

The Regulation has extra-territorial applicability, applying to controllers and processors established in the Union and for controllers and processors not established in the Union who offer goods or services to data subjects in the Union and if a controller monitor data subjects behavior within the Union.

Even though most of popular fitness wearables are under other jurisdictions, such as the United States of America and Canada, this will be irrelevant, as long as one of the criterion pursuant to Article 3 of the Regulation applies. If so, the data controllers established in another jurisdiction have to comply with the Regulation.

The provisions of the GDPR, including data portability, will also be applicable for the Member States of the EEA. While the Regulation is directly binding upon the Member States of the EU, this is not the case for EEA Contracting Parties. EU legal acts with EEA relevance needs

---

167 Ibid.
168 Garmin, “How to use Garmin Connect”.
169 Through the user profile on the Garmin connect website.
170 DC Rainmaker, “Garmin enables migration from Fitbit”.
171 GDPR, Article 3 (1).
172 Article 3 (2).
173 Article 99 (2).
to be incorporated into the EEA Agreement. The Regulation is currently an adopted act under scrutiny by the EEA. When the Regulation is incorporated into the EEA Agreement, the act will be binding upon all EEA Contracting Parties\textsuperscript{174}. Presumably, this will be in place, so the Regulation applies to all Member States when the Regulation entry into force 25 May 2018. For instance, Norway, a contracting party to the EEA Agreement, have assumed that the Regulation will be included in the Agreement, and therefore started the legislative process adopting the Regulation into Norwegian law. In Norway, due to its dualistic legal system, EU regulations cannot directly apply to Norwegian law.

4.2.2 Lawful processing

As for the applicability of the right to data portability, fitness wearables are electronic devices with the ability to connect to the internet. The three cumulative conditions will be addressed, lawful processing, personal data concerning and provided by the data subject, and the rights and freedoms of others.

Fitness wearables will commonly be used based on \textit{terms of conditions}, which is understood as a consent from the individual. However, the data collected from the devices could in many cases reveal sensitive personal data about individuals using the devices.

The Working Party discuss processing of sensitive data stating that:

Such a situation is likely to arise in the specific contexts like Quantified Self devices. In these cases, the relevant devices are mostly registering data relating to the well-being of the individual. This data does not necessarily constitute health data as such, yet it may quickly provide information about the individual’s health as the data is registered in time, thus making it possible to derive inferences from its variability over a given period\textsuperscript{175}.

4.2.2.1 Ought to be a requirement of “explicit” consent?

As discussed in the previous section, personal data may be used to reveal sensitive information about an individual. The data collected such as height, weight and gender, are being used to determine personalized fitness stats. For example, calories burned and the number of steps the individual take. Height and weight combined can be used to measure a person’s BMI. With this

\textsuperscript{174} EEA Agreement, Article 7.

\textsuperscript{175} WP29, Recent Developments on the Internet of Things, 17.
measurement, the individual is categorized as either underweight, normal, overweight or obese. The result will give an identification on the health status of individuals.

An individual using a fitness wearable, may also connect a smart scale measuring exact weight when used and could be used to analyze the difference between each time an individual measures their weight with the scale.

As de Hert and Papakonstantinou stated, even though “revealing” could denote a dynamic interpretation, this had not been proved to be the case in the past. The distinguishing is based of “its nature and not its potential uses”176. The sole purpose of the fitness wearables is so the individual can track their activities, related to chosen health data. The results of the activities collected by the device will give indication on the user’s health. A requirement of explicit consent is obviously a relevant question to be addressed by the stakeholders in the future.

4.3 Are the activities tracked by fitness wristbands personal data “provided by” the data subject?

The “activities” tracked by fitness wristbands includes geo location, pace, heartbeat and the result of continuous analyses of the data such as calories burned, sleep quality and number of steps taken.

The most prominent interpretation of “provided by” the data subject is from the Working Party. According to WP29, “data actively and knowingly provided by the data subject” and “observed data provided by virtue of the use of the service or the device”, are data “provided by” the data subject177.

“Actively and knowingly” provided by the data subject is data submitted in online forms. For fitness wearables, this will be data concerning height, weight, max pulse, and age, depending on the device. The data is manually imputed by the individuals into the service provider.

Data collected virtue of the use of the device is data such as heartbeat, geo location, steps taken, sleep quality and calories burned. The device may have a built-in geo location sensor which will track the individual while the device is turned on and in use. The heartbeat of the individuals may be measured by a wearable computing, either by the device itself or with a pulse belt. Depending on the capabilities of the device, an individual could see the heartbeat and distance live on the device. On a bicycle computer, an individual may additionally see

177 WP29, Guidelines v2, 10.
cadence and watts per hour live. After the exercise, or simultaneously, the tracked activities are analyzed to give the individual a score on the efforts used while training and/or whether the individual achieved the goal set by that individual or a chosen training program.

The individuals using fitness wearables may have different purposes. However, a common purpose for individuals measuring their activities could be to use the statistics for analyzing their training effort and/or motivation to be healthy with daily, monthly, and yearly goals. In addition, the collected data could be used by the individual to adjust their training efforts in relation to the individuals max pulse and the endurance for the exercise.

For an individual to be able to bring these data with them in a portability request, the data must concern the individual and be “provided by” him or her. The requirement of “concerning” the individual seems to be clear. A common way to access the data is to log into the service provider with a username and password. The tracked activities will be linked to that user account. Additionally, remaining anonymously using fitness wearables and similar services are not possible, as the device and the other connected devices have a range of identifiers, such as MAC addresses178.

The uncertain question is whether these activities are recognized as “provided by” the data subject pursuant to Article 20 (1). It is the data subject who activates what information that will be tracked from the device, and is the reason for the data collection by the data controller. However, it is the service provider who manages the devices and their functions. The individuals activate them. It will therefore not fall under data “actively and knowingly” provided by the data subject, but could be recognized as passively provided data.

When asserting the Working Party’s interpretation of “provided by” the data subject, this includes “observed data provided by the data subject by virtue of the use of the service or the device”. They have provided examples of what is within the scope, such as “a person’s search history, traffic data and location data [and] other raw data such as the heartbeat tracked by a wearable device”179. According to this interpretation, the heartbeat and geo-location tracked in the fitness wearable and extra optional devices connected, will be within the scope of “provided by” the data subject. The geo-location will include the distance travelled for the exercise or daily use.

However, steps taken are made on the basis of the controller’s analysis of data, for example height of the individual, pace, and the distance traveled. The analysis is different for each

178 WP29, Recent Developments on the Internet of Things, 8.
179 WP29, Guidelines v2, 10 and 11.
service providers, as seen by the different results when using the devices. Additionally, a sensor by itself does not provide the data for sleep quality and calories burned. This is also data generated by the controller’s analysis of the tracked data. These sets of data shall not be understood as “raw data”, and consequently will not be within the same scope as the geo-location and the heartbeat. They might rather be recognized as inferred or derived data. According to WP29, this is data created on the basis of the data “provided by” the data subject\textsuperscript{180}, including raw data. Inferred and derived data, “which include personal data that are created by a service provider” are according to the interpretation excluded from data “provided by” the data subject\textsuperscript{181}. There is not a discretion presented in that opinion. However, even though inferred data can be excluded from a portability request, the Working Part states that the controller should include all other personal data provided by the individual\textsuperscript{182}. The Working Party also determine that data derived or inferred from the data is for instance data processing “by a personalization or recommendation process, by user categorisation or profiling”\textsuperscript{183}. The data created virtue by the use of a fitness wearables, does not suit these data processing categories.

There is also another legal basis for excluding these data. The data controllers possess different identifiers to provide the individual with the information on calories burned and steps taken\textsuperscript{184}. For instance, the service providers have different algorithms translating the raw data into the statistics presented to the individual using the service. Such algorithms may be within the scope of trade secrets and/or intellectual property. The data controller is not obliged to provide that information in a portability request. Thus, this should be understood as easily solvable. As seen in section 4.1, some fitness wearables already provide such data concerning the individual. Within the data, the individual receives the result of such analyses, for example calories burned, sleep quality and steps taken. They do not provide the algorithms behind the data. The Working Party states that even though data controllers could exclude derived data, controllers should include all other personal data\textsuperscript{185}.

\textsuperscript{180} Ibid, 10.
\textsuperscript{181} Ibid.
\textsuperscript{182} Ibid.
\textsuperscript{183} Ibid, 10 and 11.
\textsuperscript{184} New York Times, “For Fitness Bands, Slick Marketing but Suspect Results”. The service providers do not have the same result, proven by the findings in the article.
\textsuperscript{185} WP29, Guidelines v2, 10.
5 General rules when answering data portability requests

There are some practical questions to be considered by the data controller to define the legal obligation to comply with portability requests. Literature has shown great tension between the fundamental right to data protection and the exercise of data portability, for example that “with the RDP [right to data portability], one-time access to a site, such as by a hacker, can turn into a lifetime’s download of data from that site”\(^{186}\). The actual scope of this hypothesis is highly uncertain, but it clarifies that it is essential to address the exercise of a portability request with care. For instance, service providers may have significant amounts of personal data concerning data subjects. If personal data get in the wrongs hands, it could have consequences for the individual concerned.

The general rules governing the exercise of data portability are, firstly, that the data subject needs information about their right to data portability. Secondly, the data controller must identify the data subject requesting the portability. Thirdly, the timeframe for when the data controllers are obligated to answer the request. Fourthly, whether or not the controller could charge the data subject for a portability request. And lastly, whether and how the data should be secured\(^{187}\).

5.1 The obligation to provide information on the existence of the right to data portability

A data controller must provide information when personal data are collected from the data subject\(^{188}\). In other words, to comply with the right to data portability, data controllers must inform data subjects of the existence of the right. A general principle is that the controller must be transparent to the data subject\(^{189}\).

Where the personal data relating to a data subject are collected from the data subject, the controller shall provide information of the existence of the right to data portability “at the time when personal data are obtained”\(^{190}\).

\(^{187}\) These general rules were also listed in WP29. Guidelines v2, 13-20. The rights of data subject are listed in chapter 3 of the Regulation, where article 12-14 will be covered in this section, as also covered by WP29.
\(^{188}\) GDPR, Articles 13 and 14.
\(^{189}\) The principle of lawfulness, fairness and transparency cf. Article 5 (1) (a).
\(^{190}\) Cf. Article 13 (2) (b).
Where the personal data have not been obtained from the data subject, the controller shall also provide information about the existence of the right to data portability\(^{191}\). Data controller are required to provide information “within a reasonable period”, not exceeding one month after obtaining the personal data, at the time of the first communication to that data subject, or when the controller disclose personal data to third parties\(^{192}\).

Article 12 (1) requires that data controllers “provide any information” relating to processing to the data subjects “in a concise, transparent, intelligible and easily accessible form, using clear and plain language.” Additionally, clarifying the importance of this where the information is addressed to children.

The Working Party provides for further guidance. However, this is just recommendations and is not obligations for the data controllers. WP29 advise that data controllers “always include information about the right to data portability before data subjects close any account they may have”\(^{193}\). WP29 also state “when providing the required information data controllers must ensure that they distinguish the right to data portability from other rights” particularly explaining the different types of data accessible through the rights of subject access and data portability\(^{194}\).

### 5.2 Identification of the data subject

There are no prescriptive requirements in the Regulation on how to authenticate the data subjects\(^{195}\). However, there is a general principle providing that the personal data is kept in a form which permits identification of the individual\(^{196}\). Additionally, Article 12 (2) states that the controller “shall not refuse to act on the request of the data subject” exercising his or her right to data portability, unless the controller process personal data for a purpose that does not require identification of the data subject and “demonstrates that it is not in a position to identify the data subject”\(^{197}\). If the controller is not able to identify the data subject, the controller must inform the data subject accordingly if possible\(^{198}\). There may also be circumstances where the data controller has reasonable doubts concerning the identity of the natural person requesting

\(^{191}\) Cf. Article 14 (2) (c).
\(^{192}\) Cf. Article 14(3) (a) to (c).
\(^{193}\) WP29, Guidelines v2, 13.
\(^{194}\) Ibid.
\(^{195}\) Also stated by the WP29, Guidelines v2, 13.
\(^{196}\) The principle of storage limitation, cf. GDPR Article 5 (1) (e).
\(^{197}\) Article 12 (2) cf. 11 (1).
\(^{198}\) Article 11 (2).
data portability. Where there is such a concern, the data controller may request the provision of “additional information necessary to confirm the identity of the data subject” before any data transfer has been made199.

The data subject will be able to exercise his or her right if they can provide additional information which will enable his or her identification200. Providing the additional information for identification will be up to the data subject, as the data controller in these circumstances does not have an obligation to acquire additional information themselves to identify the data subject, if the processing of personal data does not permit the controller to identify a natural person201. However, if the data subject provides additional information to support the exercise of the right to data portability, the controller should not refuse this information.202

According to Recital (57) of the Regulation, identification includes digital identification of a data subject, such as an authentication mechanism with credentials used by the data subject to log into the service offered by the data controller. As the Working Party states, “the data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing”203. When a data subject registers for online services, email accounts or on social networks, the data subject will most likely be required to provide a username and password connected to the service, where the data processing and the personal data are linked to that user account. This will according to WP29 be sufficient to authenticate the data subject204.

The data controller cannot require additional information which will lead to “excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested”205.

5.3 What is the time limit to answer a data portability request?

Article 12 (3) requires that data controllers provides “information on action taken” on the right to data portability to data subjects “without undue delay” and in any circumstance “within one month of receipt of the request”. Further extension of the time limit is possible, as Article 12

199 Article 12 (6).
200 Article 11 (2).
201 Recital (57).
202 Recital (57).
203 WP29, Guidelines v2, 14.
204 Ibid.
205 Ibid.
(3) provides for further extension up to a maximum of three months where it is necessary, taking into account the “complexity and number of requests”. However, there is a requirement provided that the data controller has informed the data subject within one month of the request about the reason for such delay.\textsuperscript{206} 

In practice, this will not be difficult for many data controllers. As WP29 discuss, the data controllers operating information society services are most likely equipped to handle such requests within a short period.\textsuperscript{207} 

Data controllers who refuse to take action on a data portability request, must inform the data subject of “the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy” without delay and no later than one month after the receipt of the request.\textsuperscript{208} Data controllers cannot remain silent when they receive a data portability request from a data subject.\textsuperscript{209} 

5.4 Could a portability request be rejected or a fee charged? 

According to Article 12 (5), any information provided by the data controller, or any actions taken under the right to data portability, shall be provided free of charge. However, this does not apply in all occasions. Where the data controller can demonstrate that the portability requests are manifestly unfounded or excessive, “in particular because of their repetitive character” a fee could be charged the data subject.\textsuperscript{210} 

Firstly, the data controller may charge “a reasonable fee” taking into account the administrative costs, and secondly, the data controller may “refuse to act on the request”.\textsuperscript{211} However, the Working Party states that there will be few cases where the data controller actually could justify a refusal to deliver the information in a data portability request.\textsuperscript{212} They argue this based on that the information society services specialized in automated processing of personal data could implement APIs which can facilitate the exchanges of the information with the data subject, which will lessen a potential burden of repetitive requests.\textsuperscript{213} Additionally, WP29 states that the

\textsuperscript{206} GDPR, Article 12 (3).  
\textsuperscript{207} WP29, Guidelines v2, 14. 
\textsuperscript{208} GDPR, Article 12 (4). 
\textsuperscript{209} WP29, Guidelines v2, 15. 
\textsuperscript{210} GDPR, Article 12 (5). 
\textsuperscript{211} Ibid. 
\textsuperscript{212} WP29, Guidelines v2, 15. 
\textsuperscript{213} Ibid.
“overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request”\textsuperscript{214}. Article 12 (5) focus on requests from one individual, cf. the wording “a data subject”. “As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests”\textsuperscript{215}.

### 5.5 Securing portable data

The processing of personal data shall ensure “appropriate security”, including “protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”\textsuperscript{216}. There is no reference in the Regulation to how the portable data should be sent, either to a new data controller or to the data subject concerned. There is a recognized risk of data security with portability requests\textsuperscript{217}. However, the principle of integrity and confidentiality pursuant to Article 5 (1) (f) applies for all processing activities of personal data.

Swire and Lagos declare that the right to data portability bear significant tension with the right to security of processing\textsuperscript{218}. The right to security of processing\textsuperscript{219} indicate that the data controller must implement “appropriate technical and organisational measures to ensure a level of security appropriate to the risk” including encryption of personal data, among more\textsuperscript{220}.

When addressing how data controllers can ensure that personal data are securely delivered to the right person, the Working Party states that:

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller is responsible for taking all security measures needed to ensure not only that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect

\textsuperscript{214} Ibid.

\textsuperscript{215} Ibid.

\textsuperscript{216} The principle of integrity and confidentiality, cf. article 5 (1) (f).

\textsuperscript{217} See WP29, Guidelines v2, 19 and 20; Swire and Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare”, 373.

\textsuperscript{218} Swire and Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare”, 373. They are referencing to the Proposal’s article 30, which is amended to article 32 of the Regulation.

\textsuperscript{219} GDPR, Article 32.

\textsuperscript{220} Article 32 (1) (a) to (d).
the personal data that remains in their systems, as well as transparent procedures for dealing with possible data breaches […]\textsuperscript{221}

Further, WP29 requires data controllers to assess specific risk linked with data portability and take appropriate risks mitigation measures. Firstly, “if the data subject already needs to be authenticated, using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password”\textsuperscript{222}. Some service providers already have a two-factor authentication to their user accounts in place. This is a method where the individual will be authenticated utilizing a combination of two different components. Some typical examples are that the individual provides a username and password, then receiving an email or text message for further authentication. The social networks Facebook\textsuperscript{223} and LinkedIn\textsuperscript{224}, and the email provider Gmail\textsuperscript{225}, have the possibility for further authentication.

Secondly, “suspending or freezing the transmission if there is suspicion that the account has been compromised”\textsuperscript{226}. Swire and Lagos states that downloading data \textit{without hindrance} will add “an additional layer” of risk, where the wording could be interpreted to “prohibit a site from double-checking a user’s identity if the request comes from a new IP address or otherwise appears to present a higher risk of identity fraud”\textsuperscript{227}. Thus, this seems to be an unreasonable interpretation of the data portability. Answering portability requests are recognized as processing activities, and data controllers have to comply with their obligations for “appropriate security”\textsuperscript{228}. Such interpretation of “without hindrance” should not limit the security of the processing of personal data. The Working Party affirms this by providing that legitimate obstacles may arise for circumstances related to the rights and freedoms of others and the security\textsuperscript{229}.

Thirdly, “in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as tokenbased authentications, should be used”\textsuperscript{230}.

\textsuperscript{221} WP29, Guidelines v2, 19.
\textsuperscript{222} Ibid, 20.
\textsuperscript{223} Facebook, What is two-factor authentication and how does it work?
\textsuperscript{224} LinkedIn, Two-Step Verification – Overview and Troubleshooting.
\textsuperscript{225} Google, Better security for your Google-account.
\textsuperscript{226} WP29, Guidelines v2, 20.
\textsuperscript{228} GDPR, article 32 (1) cf. article 4 (2) “disclosure by transmission” and “otherwise making available”.
\textsuperscript{229} WP29, Guidelines v2, 15.
\textsuperscript{230} Ibid, 20.
5.6 What if data controllers do not comply with their obligation for data portability?

Even though data controllers have an obligation to answer data portability requests where the requirements are met, there may be circumstances where the controller does not comply with its obligations. If so, the Regulation empower the data subjects to seek judicial remedy for damages and file administrative complaints with supervisory authority. I will in this part, briefly explain the mechanisms available for data subjects for controllers’ non-compliance with the obligations set by the Regulation.

Every supervisory authority has corrective powers they can impose to data controllers, for example warnings and reprimands231. Additionally, supervisory authorities can impose administrative fines pursuant to article 83232. Administrative fines could be in addition to, or instead of the measures of the supervisory authorities’ corrective powers233.

The Regulation creates a two-tiered structure of administrative fines. The maximum fines are 20 000 000 EUR or 4 % of the total worldwide annual turnover of the preceding financial year for an undertaking, whichever is higher234. For violations deemed less serious, the wording is the same as for the maximum fines, but rather 10 000 000 EUR or 2 %235. Infringements of the right to data portability are within the tier of maximum fines236.

The administrative fines shall in each individual case be “effective, proportionate and dissuasive”237. When there is an alleged infringement, the supervisory authority must take a number of factors into considerations when determining whether it should impose administrative fines, or the other measures of corrective powers238. The Recital 148 of the Regulation provides where there is a “minor infringement”, a reprimand could be used instead of an administrative fine239.

---

231 GDPR, Article 58 (2) (a) - (j).
232 This will not apply for Denmark and Estonia. However, the rules on administrative fines will be imposed by competent national courts in Denmark, and in the framework of a misdemeanour procedure in Estonia, cf. Recital 151.
233 Article 58 (2) (i).
234 Article 83 (5).
235 Article 83 (4).
236 Article 83(5) (b) cf. (2).
237 Article 83 (1).
238 Article 83 (2) (a) – (k).
239 If the controller is a natural person, a reprimand could also be chosen where the administrative fine would constitute a “disproportionate burden” cf. Recital 148.
What mechanisms may a data subject use?

Data subjects have several mechanisms they can use without prejudice to any other administrative or non-judicial or judicial remedy, as lodge complaints pursuant to Article 77, right to effective judicial remedy against a supervisory authority and a controller pursuant to Article 79, and the right to compensation and liability pursuant to Article 82.

According to Article 77 (1) of the Regulation, a data subject has the right to lodge a complaint with a supervisory authority in the Member State of the individuals’ habitual residence, place of work, or where the alleged infringement occurred. The supervisory authority is required to inform the complainant on both the process and the outcome of the complaint\(^\text{240}\). If the supervisory authority does not handle the complaint from the subject, or does not inform the data subject within three months of the lodged complaint pursuant to Article 77, the data subject can bring the proceedings against the supervisory authority before the courts of the Member State\(^\text{241}\). The right to an effective judicial remedy against a supervisory authority does also apply for legally binding decisions of a supervisory authority concerning the individual\(^\text{242}\).

Additionally, a data subject has the right to an effective judicial remedy against a controller pursuant to Article 79, where the individual considers that its rights under the Regulation have been infringed by the controllers processing of its personal data in non-compliance with the Regulation. Such proceedings against a controller must as a main rule, be brought before courts of the Member State where the controller has an establishment\(^\text{243}\). Where a data subject has suffered “material or non-material damage” as a result of an infringement of the Regulation, the individual may seek compensation pursuant to Article 82 (1). Therefore, where the controller does not comply with its obligations for the right to data portability, the data subject may seek compensation for this infringement. Additionally, the controller is liable for all damages caused by processing which infringes the Regulation\(^\text{244}\). However, in favor of the controller, Article 82 (3) provides for an *force majeure* clause stating that the controller will not be liable if the controller could not be held as responsible for the event causing the damage. Thus, this right entails the data subject to seek compensation if any damages occur in the exercise of data portability, or were a controller refuse to comply with its obligations.

\(^{240}\) Article 77 (2).
\(^{241}\) Article 78 (2) cf. (3).
\(^{242}\) Article 78 (1) cf. (3).
\(^{243}\) Article 79 (2).
\(^{244}\) Article 82 (2).
6 Conclusion

This thesis is an analysis of the legal obligations for data controllers when data subjects requests the right to data portability in Article 20 of the Regulation. This discussion included the applicability of the right, what constitutes as “provided by” the data subject, and how the general rules concerning rights of the data subject apply to the right to data portability. The analysis of the Regulation and available doctrine provide for consensus on the interpretation of the obligations for the controllers. However, the analysis also provides for some uncertainty on parts of the controllers’ obligations to comply with the right to data portability.

The latter is represented in relation the undefined terms “commonly used” format and direct transfer when “technically feasible”. Even though, the obligations for these two terms are uncertain, I argue that this will not limit data subject right to data portability in relation to its objective to give the data subjects control over their personal data245. This could rather pursue cooperation between the stakeholders in different business sectors. The wording “commonly used” indicate that it is two-folded, a commonly used format for a specific sector, and a commonly used format as a whole where there is not a common format set by the stakeholders. The obligation to comply with a direct transfer of personal data between the controllers is limited to where it is “technically feasible”. It is difficult to establish the obligation on controllers to ensure a direct transfer, as there seems not to be a clear obligation to establish an export-import-module, or anything resembling it, provided by that the Regulation does not create an obligation for controllers to have technically compatible systems246.

The applicability of the right to data portability have especially three questions in relation to data controllers’ obligations, presented in the doctrine; 1) transfer of personal data concerning more than one individual, 2) what personal data is understood as being “provided by” the data subject, and 3) circumstances where the data controller has intellectual property or trade secrets.

When a data controller complies with a portability request, the data portability must not adversely affect the rights and freedoms of others247. Thus, this circumstance will most cases relate to the data controller receiving the personal data. The receiving controller could infringe upon this obligation if it is processing the personal data for other purposes than the processing of the sending controller and does not let the third party be able to exercise its rights as a data...

245 Recital 68.
246 Ibid.
247 Article 20 (4).
subject\textsuperscript{248}. Such restriction on the purpose of the processing of personal data is also provided by the principle of purpose limitation\textsuperscript{249}.

In relation to the determination of the provision “provided by” the data subject, this establish what circumstance the individual have control over its personal data. As the right to data portability covers service providers that collect personal data in various ways, there is a need for a legal understanding of the scope of “provided by”. No matter what service the individual use, whether it is social networks or fitness wearables, there will be different categories on how the personal data are collected. This can for example be categorized as data actively and passively provided by the data subject, and I would argue that personal data within these categories are within the scope of “provided by”.

Firstly, there is data actively provided by the individual. This should be understood as any personal data which are actively and knowingly provided by the data subject. There is consensus in the literature, that this is within the scope of the RtDP. It is clear that information provided in online forms are included. The Working Party have provided for a not extensive list, which includes mailing address, user name and age\textsuperscript{250}. However, I argue that this list will also include circumstances where there is an indication of a knowingly act from the data subject in providing personal data. By this I mean that situations where individuals upload photos on social networks, send e-mails, make interpersonal messages, and so forth. Most of the personal data are created when using a service. I argue that individuals are actively and knowingly providing personal data in some extent when they are using a service, and not just with online forms.

Secondly, most of the personal data concerning an individual, is created when an individual uses a service. This provides for the relevance of passively provided personal data by the data subject. I emphasize that the meaning of passively, is the same as the Working Party defines as observed data by the data subjects use of a service. It is also widely accepted in the literature that this should be included in the wording of “provided by” the data subject. The Working Party states that for example “a person’s search history, traffic data and location data [and] other raw data such as the heartbeat tracked by a wearable device”\textsuperscript{251}, are within the scope of “observed data”. This category of data is being collected when the individual uses a service, but the individual does not have the same active approach to this kind of data, as for the actively and knowingly provided data. When providing why these data have a significant importance in

\textsuperscript{248} WP29, Guidelines v2, 11 and 12.
\textsuperscript{249} GDPR, Article 5 (1) (b).
\textsuperscript{250} WP29, Guidelines v2, 9.
\textsuperscript{251} WP29, Guidelines v2, 10 and 11.
data portability, a good example is the specter of Internet of Things, like fitness wearables. Most of the collected personal data will be within this category. It bears similarities with all other devices within the specter of Internet of Things.

If “provided by” is interpreted more narrowly, it will most likely infringe upon the purpose of the right to data portability to empower the data subjects control over their personal data\(^{252}\). The right to data portability has clearly an objective to let the individuals reuse their data and take with them data from one controller to another data controller. A narrow interpretation will include data which is not difficult for the individual to provide for again, such as name, email address, username and age. The time-consuming data, which consequently will act as a barrier for an individual to switch to another data controller, are the other actively and knowingly provided personal data, along with the passively provided data.

Another point addressed in the literature regarding data portability, is how the controllers’ obligations to comply with data portability would be if the data will be in conflict with data controllers trade secrets and intellectual property. Guidance is found where the Working Party states that inferred and derived data could be excluded from a portability request. This includes for example algorithms and statistical results. Even though trade secrets and intellectual property are not explicitly rooted in the wording of the right to data portability per se, scholars and the Working Party rely on that the RtDP is understood as an extension of the right of access, and therefore such conflict is covered by Recital 63. The wording “others” indicate that the rights and freedoms of all parties involved must be addressed, not just data subjects\(^{253}\). It should be clear that the data controller is not obligated to include data that constitutes as trade secrets and intellectual property, but they ought to include all other data required under the right to data portability.

It is clear that non-compliance and infringements with the rights presented in Regulation could result in remedies, liability and penalties for the data controllers. This could act as an important incentive for the facilitation of an effective right to data portability for individuals, and ensure the harmonization of data protection on data portability across the Member States.

### 6.1 Further research

Some further research that could have been made when writing this thesis or at a later stage, could have been to research the demarcations addressed in chapter 1.4, for example comparing the RtDP with competition law and the proposed Directive on certain aspects concerning

\(^{252}\) GDPR, Recital (68).

\(^{253}\) Article 20 (4).
contracts for the supply of digital content. Further, addressing the special characteristics of Internet of Things and cloud computing. Another possible comparison, could be the right to data portability and the payment service providers obligation to enable access to accounts by third parties by the request of the customer in the EU Payment Services Directive (PSD2).

Additionally, analyzing possible restrictions on the right to data portability pursuant to Article 23 and derogations pursuant to Article 89 made by Member States, which could limit the data controllers’ obligations for some specific processing activities. For example, the proposed exclusion in Norway for processing personal data solely for archival purposes in the public interest\(^\text{254}\).

\(^{254}\) The Norwegian Ministry of Justice and Public Security, “Høringsnotat” (Consultation Document), 129.
# Table of reference

## Statutes

AGREEMENT ON THE EUROPEAN ECONOMIC AREA (Updated 1.8.2016) (OJ NO L 1, 3.1.1994).


DIRECTIVE (EU) 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995).

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011).


TREATY OF LISBON AMENDING THE TREATY ON EUROPEAN UNION AND THE TREATY ESTABLISHING THE EUROPEAN COMMUNITY (2007/C 306/01)

## Court decisions

Judgment of the Court of 19 October 2016. Patrick Breyer v Bundesrepublik Deutschland. Case C-582/14.

Publications from authorities


The Norwegian Data Protection Authority. “Høringsuttalelse fra Datatilsynet – utkast til ny personopplysingslov – gjennomføring av personvernforordningen i norsk rett,”

Books


Articles in electronic journals


**Other secondary sources**


Web pages


