The perceived need and potential impact of Article 35, on database protection and data portability, in the proposed EU Data Act

Xueyan Shen

Master's Thesis in European and International Trade Law

HARN63

Spring 2022

Supervisor: Johan Axhamn

SCHOOL OF
ECONOMICS AND
MANAGEMENT

Table of Contents

FORWARD……6

ABBREVIATIONS……7

1. Introduction……8

1.1 Background…….....8

1.2 Purpose and research questions…….10

1.3 Delimitation…….....10

1.4 Materials and method……11

1.5 Structure…….....13

2. The GDPR and the right to data portability……14

2.1 Introduction……14

2.2 The brief introduction of the GDPR……...14

2.3 Right to data portability under the GDPR……...15

2.3.1 The concept of ‘personal data’…….15

2.3.2 Scope of the right to data portability…….....17

2.3.3 Conditions for the right to data portability……...19

(a) Prerequisites: processing based on consent or contract……..20

(b) Form: processing by automated means……...20

(c) Data conditions: personal data ‘concerning’ and ‘provided by’ the data subject…….....21

2.3.4 The exception of rights and freedoms of others……....25

2.4 Summary…….26

3. The relations between Personal Data and Sui Generis Database Right..27

3.1 Introduction…….....27

3.2 The EU Database Directive 96/9…….....27

3.2.1 The brief introduction of Database Directive…….....27

3.2.2The concept of ‘database’…….....28

3.2.3 The sui generis database right……..30

(a) Requirements of protection……..30

(a.i) Substantial investment…….....30

(a.ii) Investment in obtaining, verifying or presenting…….....31

(b) Ownership or authorship…….....33

(c) Scope of protection……..33

(d) Exceptions and limitations……..36

3.3 Connections between the right to data portability and the sui generis database right……....37

3.3.1 The controller of data and the owner of database…….37

(a) Online Platforms…….37

(b) Connected Devices…….39

3.3.2 How is the intersection between data portability and the sui generis database right……...41

3.4 Summary……..42

4. The Potential Impact of Art.35 in EU Data Act……..43

4.1 Introduction…….....43

4.2 The background of Art.35 in EU Data Act……..43

4.2.1 The EU Data Act……...43

4.2.2 The relationship between Art.35 and data portability……...45

4.2.3 The relationship between Art.35 and database protection……45

4.3 What is ‘data obtained from or generated by the use of a product or a related service’…….….....48

4.3.1 Analysis……..48

4.3.2 Examples……50

4.4 The potential impact of Art.35 in EU Data Act……52

4.4.1 The potential impact on Right to Data Portability…….52

4.4.2 The potential impact on Sui Generis Database Right……53

4.5 Summary……..54

5. Conclusion…….55

Bibliography…….57

Cases……..61

Abstract

After the proposed EU Data Act was released in February this year, the facilitation of data sharing was emphasized, which might bring many aspects of impact. In particular, the implications for data portability and database protection. The purpose of this thesis is to describe and analyze the intersection between the EU sui generis database right and the EU right to data portability, and to which extent Art.35 in the proposed EU Data Act might have an impact on these two rights. This thesis concludes that the proposed EU Data Act might extend the scope of application of the EU right to data portability and release some certain data from the EU sui generis database right. But this thesis does not consider these implications to be black or white. It hopefully draws more attention to the intersections of these two rights.

Keywords: General Data Protection Regulation, Right to Data Portability, Sui Generis Database Right, proposed EU Data Act, database protection

Foreword

I would like to firstly express my gratitude to my supervisor, Johan Axhamn. I would like to thank him for his encouragement and all the careful guidance I have received for this thesis, which has enabled me to complete it. He has inspired my strong research interest in intellectual property and has made me determined to continue my research in this field.

Secondly, I would like to thank all my friends who provided comments for my thesis during the time I was writing it. I would also like to thank my friends and families who helped me to relieve the stress of my studies and make my life better during this period. Your help has also been an indispensable motivation for me to complete this thesis.

Finally, thank you to all the singers I have listened to. Your songs have been with me every day, through all my joys and sorrows. These songs have become part of the background music of my life.

Abbreviations

EU	European Union
GDPR	General Data Protection Regulation
RtDP	Right to Data Portability
SGDR	Sui Generis Database Right
Directive 96/9	Database Protection Directive 96/9/EC
CJEU	Court of Justice of the European Union
WP	Data Protection Working Party

1. Introduction

1.1 Background

Nowadays data has been acknowledged as an essential resource for economic growth.[1] As a part of its Digital Single Market Strategy, the European Commission committed to develop a European data economy.[2] In 2016, the EU took the first step towards enhancing the internal market dimension of data. By reforming its data protection framework, including the adoption of the General Data Protection Regulation on the processing of personal data and its free movement.[3] At the same time, there is a large proportion of the data circulating in the digital economy, which is data relating to identified or identifiable natural persons, and constitutes 'personal data' within the meaning of EU data protection law. In this context, the new GDPR introduced a regulatory innovation - Right to Data Portability in relation to personal data.[4] It can be found in Art. 20 of the GDPR, which gives data subjects the right to receive and transfer their personal data, by means of copying and sharing.

As a right established within the data protection legislation, the RtDP's first and

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building a European Data Economy, COM (2017) 9 final (Jan. 10, 2017).
[2] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a Digital Single Market Strategy for Europe 14, COM (2015) 192 final (May 6, 2015).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ 2 119/1 (General Data Protection Regulation--GDPR).
[4] Graef, Inge and Husovec, Martin and Purtova, Nadezhda, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law (December 15, 2017). German Law Journal 2018, vol. 19 no. 6, p. 1359-1398, Tilburg Law School Research Paper No. 2017/22, TILEC Discussion Paper No. 2017-041, Available at SSRN: https://ssrn.com/abstract=3071875 or http://dx.doi.org/10.2139/ssrn.3071875

main objective is to grant individual a greater control over their personal data.[5] However, due to the broad wording of the GDPR, e.g. Art. 20(4) the GDPR does not explicitly state whether 'rights of others'[6] include intellectual property rights. It leads to a potential 'Silent Conflict'[7] between Sui Generis Database Right (SGDR) and RtDP. The reason is that databases are generally regarded as collections of data and SGDR protects the database owner's investment in the database by granting the owner the right to prevent the extraction and re-utilization of all or a substantial part of its contents.[8] In this context, if a data subject can exercise the right to data portability under Art. 20 of the GDPR and wishes to receive a copy of personal data relating to him or her and to transmit such data to another data controller, this would potentially intersect with the rights granted to the database owner by SGDR. Meanwhile, when data subjects are free to transfer data collected by one database maker to another, the database maker's investment in obtaining data could be reduced, which might directly challenge the principle of SGDR.

Against this background, the proposed Regulation on harmonized rules on fair access to and use of data - also known as the Data Act - was adopted by the Commission on 23 February 2022.[9] As a key pillar of the European data strategy, the proposed Data Act will ensure fairness by setting up rules regarding the use of data generated by Internet of Things (IoT) devices. Further, the proposed Data Act aims to ensure consistency between data access rights, which are often developed for specific situations and with varying rules and conditions. Based on the explanatory memorandum of the proposed Data Act, it can be seen that it consistently follows the purposes and aims of the data portability to promote data

[5] Elfering, Stephanie, Unlocking the Right to Data Portability: An Analysis of the Interface with the Sui Generis Database Right. 10.5771/9783748902706.(2019)
[6] Art. 20(4) GDPR Right to data portability, "The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."
[7] Graef, Husovec and Purtova (n 4) p10.
[8] Art. 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20.
[9] European Commission, "Shaping Europe's digital future", https://digital-strategy.ec.europa.eu/en/policies/data-act. last accessed 25th May 2022.

sharing. Thus, even if Art. 35 does not explicitly refer to the RtDP, but only to SGDR and Art. 4 and Art. 5 of this regulation. It could be considered as complementary to the existing RtDP, as long as the relevant data in the Art. 4 and Art. 5 qualify for the RtDP. For this reason, the Art. 35 might clarify the role of the database protection and data portability. And might ensure that the balance between the interests of data controllers and users is in line with the broader objectives of the EU data policy.

1.2 Purpose and research questions

The purpose of this thesis is to describe and analyze the intersection between the EU sui generis database right and the EU right to data portability, and to which extent Art.35 in the proposed EU Data Act might have an impact on these two rights.

Research questions are as follow:

1. What is the intersection between the EU sui generis database right and the EU right to data portability?
2. What is the potential impact by Art.35 in the proposed EU Data Act, in relation to the EU sui generis database right and the EU right to data portability?

1.3 Delimitation

The first half of this thesis will be devoted to the intersection between RtDP and SGDR, leading up to The Data Act's contribution to solving this intersection. This intersection can be seen as an intersection between the right of data subjects to transfer their personal data and the interest of data controllers to protect their investment in databases.

Admittedly, before the RtDP was determined to be an independent right in the GDPR, the European Parliament's review had incorporated it into Art. 15(2a)

regarding the Right of Access[10], and this incorporation implicitly indicated the Parliament's view that the RtDP was an extension of the right of access.[11] However, as the RtDP is now an independent right, and the data access right is more focused on accessing data than moving the data. The RtDP, which likely involves data extraction and reproduction behavior, is more likely to intersect with the SGDR, which is the focus of this research. So this thesis will not elaborate on data access right.

1.4 Method and Materials

In order to answer the research questions while pursuing the purpose, this thesis will gather both binding and non-binding materials. The binding materials will mainly be used to support the legal dogmatic method, in particular, EU legal method, and the non-binding materials will be cited to support personal opinion or to enrich different perspectives.

1.4.1 Legal Dogmatic Method

The 'legal dogmatic method' is used in this thesis to provide legal analysis and descriptions of legal sources.[12] Further, this legal method requires a more regional and sector-specific legal method in explaining the issues of this thesis. In this thesis, it is mainly reflected in the EU legal method.

The EU legal sources in this thesis are:

a) Directives, such as EU Database Directive 96/9[13], for describing the SGDR; and Directive 2006/24, as a reference, in the analysis of 'data obtained from or generated by the use of a product or a related service'.

---

[10] European Parliament, "Report on the 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)" A7- 0402/2013, amendment 111.

[11] Graef, Husovec and Purtova (n 4) 4.

[12] Jan M Smits, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' in Rethinking Legal Scholarship: A Transatlantic Dialogue (eds, van Gestel, Micklitz & Rubin, Cambridge University Press 2017) 207.

[13] Directive 96/9/EC.

b) Regulations, such as EU Regulation 2016/679[14], for describing the GDPR and the RtDP; and the proposed EU Data Act, for describing and analyzing the Art.35 of EU Data Act.

c) Preambles to the directives and regulations, to point out the prevailing philosophy of these instruments and the backgrounds.

d) Case law from the CJEU, which is also the material of the teleological interpretation method. When the wording or context of the law is unclear, it requires the CJEU to interpret the law in the light of its original objective. This is the core of understanding EU law. Legal interpretations made by the CJEU through case law are binding on national courts and lead to consistency of interpretation. Careful case studies can help with understanding the directives and regulations in a more greater and real-life context. The selected cases are related to data in databases protected by SGDR. The British Horseracing and Fixtures Marketing cases are used to argue from the opposite side that Art.35 of the EU Data Act will have an impact on SGDR. Other cases are cited for bringing examples to the analysis of 'data obtained from or generated by the use of a product or a related service'.

e) Opinions by the Advocate Generals, as a complement to the case study, providing a different perspective.

f) Guidelines and communications from the commission. These materials are non-binding materials and will be used to explain the background and the history of related rights and for a better description of the directives and regulations.

1.4.2 Secondary Sources

Legal literature, including books (and ebooks), journals, articles (and e-articles) and blogs of legal organizations[15] from scholars, as an important complement to different views.

[14] Regulation (EU) 2016/679 (General Data Protection Regulation).
[15] For example, the Data Protection Working Party.

1.5 Structure

Chapter 2 introduces the GDPR and The Right to Data Portability. In this chapter, it will be shown that the GDPR encourages the sharing of data. And this chapter will clarify the requirements for personal data that can satisfy the requirements of RtDP adoption. In the end of this chapter, the main reasons for the difficulties in adopting RtDP in practice will also be described.

Chapter 3 explains and analyzes the SGDR and the relationship between data portability and database protection. Before explaining this intersection, this chapter will first describe the circumstances that online platforms and connected devices bring to this intersection. The chapter will then describe how data portability threatens investments in databases. And how RtDP infringes on the exclusive rights of database makers in SGDR.

Chapter 4 follows on the previous analysis of the intersection between the RtDP and SGDR, and adds an analysis of the proposed EU Data Act. Chapter 4 will begin by explaining the relationship between Art. 35 and data portability and database protection. Then the scope of application of Art.35 will be discussed through case study. Before the end of this chapter, the potential impact of Art.35 on Right to Data Portability and Sui Generis Database Right will be analyzed respectively.

Chapter 5 is a conclusion. The research questions will be answered in this chapter.

2. The GDPR and The Right to Data Portability

2.1 Introduction

This chapter will provide an introduction to the GDPR. The focus will be on describing and analyzing the RtDP, around the concept of personal data, scope, conditions and exceptions of the right to data portability.

2.2 The Brief Introduction of the GDPR

As the internet is becoming one of the most important ways of sharing information about society, the demand of internet users to control their data has become more pressing.[16] In order to stop unfair competition[17]and protect personal data, especially in a cloud-computing era, EU Database Directive 96/9 on the protection of individuals with regard to the processing of personal data was adopted in 1995.

However, the world has changed profoundly as a result of rapid technological development and globalization, which created new challenges for the protection of personal data. And the Database Protection Directive was unable to prevent a fragmentation in the way data protection is implemented across the EU, which has led to legal uncertainty and a crisis of public confidence with regard to the privacy

[16] Kevin Allison, "Social networks may find it does not pay to be too possesive" .Financial Times, 21 January 2008; available online at ,http://www.ft.com/intl/cms/s/0/8b6351e4-c843-11dc-94a6-0000779fd2ac.html#axzz1lM5qQASD. accessed 14 April 2022. (state that data portability appeared as a way that would enable the widespread sharing of social information between websites)

[17] Randal C. Picker, "Competition and Privacy in Web 2.0 and the Cloud" (2008) 414 John M. Olin Law & Economics Working Paper; Jasper P. Sluijs, Pierre Larouche, and Wolf Sauter, "Cloud Computing in the EU Policy sphere" (2006) 036 TILEC Discussion Paper. Although both papers are focusing on cloud computing, the data portability dimension leading to fair competition practices is also tackled.

risks of online activities.[18]

To prevent a lack of consumer confidence from discouraging the adoption of new digital products and services, resulting in a lack of incentive to innovate.[19] The GDPR emerged, which is intended to strengthen the rights of individuals to control their data.[20] Not only for the choice of secondary law,[21] but also for the new rights it introduces for data subjects. The GDPR is considered as a truly innovative and revolutionary piece of legislation.[22] As only the new rights introduced by the GDPR are relevant to this paper, the following will focus only on this respect. The new rights that data subjects are complemented with are: (i) the right to erase[23] (or right to be forgotten), and (ii) the RtDP[24]. As these two rights are independent of each other, only the RtDP will be discussed separately below.[25]

2.3 The Right to Data Portability under the GDPR

2.3.1 The Concept of 'Personal Data'

The definition of 'personal data' is essential for determining the GDPR's scope, so before analyzing the RtDP, the definition of 'personal data' will be discussed in detail.

According to Art.4(1) GDPR, the 'personal data' means any information relating

[18] European Commission, Special Eurobarometer (EB) 359, "Data Protection and Electronic Identity in the EU"(2011),http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. accessed 14 April 2022.
[19] Graef, Husovec and Purtova (n 4) p10.
[20] COM(2010) 609. p5.
[21] "Under the DPD, significant divergences were verified across Member States' national data protection laws. The GDPR solves this problem by defining its territorial scope as EEA." COM(2010) 609. p3; SEC(2012) 72. p11.
[22] Banda, Carolina, "Enforcing Data Portability in the Context of EU Competition Law and the GDPR"(September 13, 2017). MIPLC Master Thesis Series (2016/17).p61, 28; Graef, Husovec and Purtova (n 4) p149, 150.
[23] GDPR art. 17.
[24] GDPR art. 20.
[25] WP art. 29. (state that these are two independent rights under the GDPR, when the RtDP is invoked, it does not automatically trigger a request for erasure)

to an identified or identifiable natural person ('data subject').[26] Within this concept, the 'identifiable natural person' means one who can be identified, directly or indirectly by reference to an identifier of that natural person. For identifiers, Art.4 lists obvious identifiers such as name and ID, as well as examples of exceptions such as gender and culture.[27] Articles 4(13) to (15) GDPR further define three special categories of personal data as (i) genetic data; (ii) biometric data; and (iii) data concerning health.[28]

According to the broader interpretation of personal information in case law, the CJEU held the view that even a dynamic IP address could constitute personal data, as the controller could obtain additional information to identify the data subject.[29] The Recital 26 GDPR[30] provides further guidance by adopting a 'test of reasonable likelihood of identification'.[31] In this test, all means reasonably likely to be used by the controller or a third party have to be considered. In addition, all objective factors should be taken in order to ascertain whether means are reasonably likely to be used, such as the cost and time required for identification in the case of existing technology.

And now, with the Nowak case[32], the CJEU has expanded the interpretation of 'personal data' to the scope of subjective information:

> [T]he expression 'any information'(.....) reflects the aim of the EU legislature to assign a wide scope to that concept [of personal data], which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not

[26] GDPR art. 4.
[27] GDPR art 4(1), the obvious identifier such as a name, an identification number, location data, an online identifier. Additional examples are the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
[28] GDPR art. 4.
[29] Case C-582/14 Breyer [2016] ECLI:EU:C:2016:779 para 44-49.
[30] GDPR recital. 26.
[31] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) Law, Innovation and Technology 10 (1). p40, 44.
[32] Case C-434/16 Nowak [2017] ECLI:EU:C:2017:994 para 62.

only objective but also subjective.[33]

According to the previous section, 'personal data' might include any kind of information. Except anonymous data[34], the non-personal data[35] and pseudonymous data[36] can also be personal data when its combination with other data can achieve the effect of identifying an individual.[37] And with the development of Internet technology, there is reason to believe that personal data will become a progressively broader concept.

2.3.2 Scope of the Right to Data Portability

The scope of the right to data portability refers to two rights vested in the data subject by the RtDP, which are：(i) the right to receive and transfer personal data[38] (indirect portability), and (ii) the right to have it transmitted directly from one controller to another[39] (direct portability). RtDP therefore means that data subjects have the freedom to 'copy' and 'share' their own personal data, and the use of RtDP results in the personal data existing with both the first controller and the data subject and/or the second controller.

Firstly, the indirect portability, which is also two-folded -- It allows data subjects (i) not only to receive their personal data, (ii) but also to transmit this data to another controller without being hindered by the original controller. It may be more clear to understand this right from the perspective of the controller, which

---

[33] Ibid para 34.

[34] According to recital 26 GDPR , 'anonymous data' means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

[35] According to article 3(1) Regulation (EU) 2018/1807, 'Non-data' means data other than personal data as defined in point (1) of Art.4 of Regulation (EU) 2016/679.

[36] According to Art.4(5) GDPR, 'pseudonymisation' means 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[37] According to recital 26 GDPR ,'personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person'.

[38] GDPR art 20(1).

[39] GDPR art 20(2).

means:

Assisting data subjects in implementing the indirect portability, the controller must provide the data in a 'structured, commonly used and machine-readable format', such as an interoperable format[40]. This means that the format should at least enable the individual or another controller to reuse the data.[41] And according to the EU Database Directive 96/9[42], 'the machine-readable format' requires the data to be in a file format, which is structured so that software applications can easily identify, recognize and extract specific data from it. However, the provision also clarifies that 'documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format', such as a PDF file.[43]

What is more, the first controller may not impose any hindrance when the data subjects transmit their personal data to another controller. And according to the WP29 Guidelines, a hindrance is 'any legal, technical or financial obstacles placed by data controller to refrain or slow down access, transmission or reuse by the data subject or by another data controller'.[44]

Secondly, the direct portability. As it requires an additional requisite -- 'technically feasible'[45], which also makes it considered to be a strong argument

---

[40] According to recital 68 GDPR, "To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller."

[41] COM(2012) art. 18(1); WP art.242(state that it should allow 'for further use [of the data] by the data subject' ' They are minimum requirements to enable reuse of the data by the individual or another controller')

[42] Directive 2013/37/EU

[43] WP art.242 p18. (state that a PDF file was not considered machine-readable by WP29)

[44] Ibid p15.

[45] According to article 20(2) GDPR,'In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.'; According to recital 68 GDPR, 'Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.'

for the controller to avoid the portability request sometimes.[46]

Although the GDPR does not define or explain what is 'technically feasible', in line with the consistent interpretation of the context of the law and the Commission's proposal[47]. The 'technically feasible' should meet the basic requirement that the transmitting and receiving data processing systems can communicate, i.e. be interoperable. However, Recital 68 GDPR does not make 'technologically feasible' an obligation for controllers, it clearly states that "RtDP should not create an obligation for controllers to adopt or maintain processing systems which are technically compatible".[48] In view of this provision, which contains only an encouragement[49] but not an legal obligation, the likelihood of the data subject's use of direct portability is considerably limited.

Under the WP29 proposal, 'technical feasibility' should be assessed on a case-by-case basis.[50] So it is currently not clear in which cases the data subjects can actually use the right of direct portability. But the data subjects still have the right to indirect portability and there is nothing to prevent them from subsequently transferring the data to another controller. This is merely clearly not conducive to reducing the data subjects' transfer costs.

2.3.3 Conditions for the Right to Data Portability

According to Art. 20 GDPR, if the data subjects intend to use their right to data portability, the following three conditions must be fulfilled at the same time: (i)

---

[46] Vanberg AD and Ünver MB, "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?"(2017) 8 (1) EJLT. p4.(state that the likelihood of controllers refusing to comply with portability requests based on technical unfeasibility cannot be underestimated; In cases where the controller is unwilling to share the individual's personal data with a third party this might seem a good way to circumvent the obligation, undermining the RtDP's purpose)

[47] COM(2012) 11 art 18(1), " it should allow 'for further use [of the data] by the data subject".

[48] According to recital 68 GDPR, "The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible."

[49] According to recital 68 GDPR, "Data controllers should be encouraged to develop interoperable formats that enable data portability."

[50] WP art.242. p16; WP art.29 understands the 'technical feasibility' concept as (i) a secured communication system between the transferring and receiving controllers, as well as (ii) the capability of the receiving controller's system to receive the incoming data.

processing must be based on consent of the data subject or a contract[51], (ii) the form of processing must be by automated means[52] and (iii) the object of the processing must be personal data which is provided by and concerning the data subject[53].

(a) Prerequisites: Processing Based on Consent or Contract

According to Art. 20 GDPR and the relevant articles[54], the prerequisites for personal data to be processed for the purpose of RtDP are (i) the data subject's consent, or (ii) a contract between the data subject and the transferring controller. Any other data processing that base on other legal ground is excluded from the RtDP's application. The solely legal ground makes the impact of RtDP strongly limited. For example, RtDP is not applicable when the processing of data is based on 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'[55] or 'legitimate interest'[56]. Considering balancing interests of the controller with other rights and interests of others[57], WP29 recommended personal data portability to be adopted as a good practice, even in non-mandatory cases.[58]

(b) Form: Processing by Automated Means

According to Art. 20(1)(b) GDPR, the RtDP applies only where the processing is

---

[51] According to art 20(1)(a) GDPR,' the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)'

[52] According to art 20(1)(b) GDPR,'the processing is carried out by automated means'

[53] According to art 20(1) GDPR,'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'

[54] According to art 6(1)(a)(b) GDPR,'Processing shall be lawful only if and to the extent that at least one of the following applies: (a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'; According to art 9(2)(a) GDPR,'Paragraph 1 shall not apply if one of the following applies: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject'

[55] article 20(3) and recital 68 GDPR

[56] article 6(1)(f) GDPR,'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

[57] WP art.29, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC," April 9, 2014, WP art.217.

[58] WP art.242. p8.

‘carried out by automated means’, this provision limits the forms of processing data. However, there is no clear definition of ‘automated means’ in GDPR, according to relevant studies, ‘automatic’ is regularly expressed as processing ‘by a computer’[59] or ‘through technology’[60]. It is reasonable to assume that ‘automatic’ leads to ‘operable by machines and computers’, which is consistent with the understanding of most scholars.[61]

What is more, through the analysis of the Recital 15 of GDPR, it seems possible to assume that ‘automated means’ should not include ‘manual processing’, i.e. processing by individuals. As ‘automated means’ is a different type of data processing from ‘manual processing’.[62] This categorization is also supported by the WP29, which considers that paper files should be excluded from ‘automated means’.[63]

(c)Data Conditions: Personal Data ‘Concerning’ and ‘Provided by’ the Data Subject

After analyzing Art. 20(1) GDPR, this provision in fact contains three requirements: firstly, the data are concerning the data subject; secondly, the data are personal data; and finally, the data are provided by the data subject.

First of all, the description -- ‘personal data concerning the data subject’ is ambiguous and can only exclude data that is exclusively related to other data subjects. In reality, data is always intertwined, a single piece of data is likely to relate to more than one data subject at the same time, and it may not be possible to

---

[59] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, “Realising the Right to Data Portability for the Domestic Internet of Things”.(2017) , p3 <https://ssrn.com/abstract=2933448> accessed 18 May 2022.

[60] Paul Voigt and Axel von dem Bussche, “The EU General Data Protection Regulation (GDPR): A Practical Guide” (2017) Springer. p10.

[61] Elfering, Stephanie, (n 5) p25-26.

[62] recital 15 GDPR ‘Technology Neutrality’:‘The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.‘ In explaining the protection of natural persons in data processing, this provision uses the term "as well as" to divide data processing into two categories, those processed in an automated means and those processed manually, so it can be understood that the GDPR treats automatic processing and manual processing as two different types.

[63] WP art.242. p9.

extract solely personal data that relates to only one of these data subjects. In this case, if the scope of 'concerning' is not reasonably defined, a dilemma arises. Overly strict requirements that require personal data relating exclusively to the data subject may result in the inability to divide the data or the loss of data value. For example, if only the part of the video relating to the data subject is extracted and the part relating to other data subjects is left, the video may become a meaningless fragment. However, if the integrity and value of personal data is preserved, then there will be a high risk of infringement of other data subjects' rights to this data.

Recital 68 and Art.20(4) GDPR implement the principle of GDPR that protects the interests of data subjects, so this recital outsets and extends the scope of 'concerning' to not infringing on the rights and freedoms of other data subjects.[64] And the WP29 also recommended not to adopt an overly strict approach in line with Recital 68 GDPR. If the processing of the receiving controller would not adversely affect the rights and freedoms of any of the other data subjects, the transmission controller shall transfer the data.[65]

Secondly, the data that can be the object of RtDP have to be the personal data, which means the relevant data can identify the data subject. Non-personal data and pseudonymous data can be personal data where certain conditions are met, while anonymous data is excluded. As the analysis of 'personal data' has already been discussed in detail, it will not be repeated here.

Last but not least, Art. 20 GDPR requires that only the data provided by the data subject can be the object of RtDP. This provision significantly limits the availability of RtDP and undermines the original purpose of RtDP in preventing

[64] recital 68 GDPR, 8th sentence reads as follows: 'where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation'.
[65] WP art.242. p9.

lock-in effects. Because data concerning data subjects provided by third parties to the controller is excluded, and it is not conducive to reducing barriers for customers to transfer data between different providers.[66]

As with the aforementioned 'concerning', there arose a great controversy due to the fact that different interpretations of the scope of 'provided by' can have a huge impact on the scope of application of the RtDP.[67] If adopting a restrictive interpretation of 'provided by', it refers to data explicitly provided by the data subject to the data controller; if adopting a broad interpretation, it refers to all data collected by the data controller with the consent of the data subject or in the framework of a contract, including 'observed data'.[68]

The controversy about the scope of 'provided by' stems mainly from the classification of personal data based on their origin.[69] According to this classification, there are four different categories of personal data, each of these will be analyzed below:

(i) 'provided data', which is actively and knowingly disclosed by the individual, for example, posting on social media. There is no dispute about this type of personal data, as it falls precisely within the scope of application of the RtDP.

(ii) 'observed data', which is observed from the individual and recorded by a third party, for example, sensors such as smart wearables used for mobile health care, checking the bodily functions of a patient. Although there are some

---

[66] Elfering, Stephanie, (n 5) p52; WP art.242. p5; Graef, Inge, "Data as Essential Facility: Competition and Innovation on Online Platforms" (2016). p154-155.(state that the rationale behind the RtDP was precisely to reduce consumer lock-in, by enabling individuals to take their personal data and switch providers more easily. Competition and innovation in the data economy were expected to be concomitantly promoted, as portability reduces entry barriers for personal data dependent business models)

[67] Paul De Hert, Vagelis Papakonstatinou, Gianclaudio Malgierei, Laurent Beslay and Ignacio Sanchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services"(2018) Computer Law and Security Review. p7; Graef, Husovec and Purtova (n 4) p9; Gianclaudio Malgieri, "User-provided personal content in the EU: digital currency between data protection and intellectual property"(2018) 32 (1) IRLCT. p118, 130.

[68] Paul De Hert, Vagelis Papakonstatinou, Gianclaudio Malgierei, Laurent Beslay and Ignacio Sanchez, (n 66)p34 (state that these as the only two possible interpretations)

[69] This classification was first discussed in 2014 within the Organisation for Economic Co-operation and Development (OECD). OECD, "Summary of the OECD Privacy Expert Roundtable on 21 March 2014 - Protecting Privacy in a Data-driven Economy Taking Stock of Current Thinking"(2014) DSTI/ICCP/REG. p3, 5.

arguments about whether personal data passively provided under this category can be the object of RtDP, with some scholars arguing that 'provided by' should describe an active act.[70] Other scholars have argued that when personal data is collected from a connected device, the data subject is in fact actively and knowingly using the device, which means that he acquiesces to his personal data being provided to the controller by the device.[71] In addition, excluding personal data observed and recorded by a third party and passively provided by the data subject contrary to the purpose of the RtDP, which is to provide individuals with greater control over their own data in the data economy.

(iii) 'derived data' , which means new data generated based on other data from the individual, for example, computational and notational data. The difference between this type of data and 'provided data' and 'observed data' is that 'derived data' is not readily available. Whether the new data is created by the data subject in the course of using the product or service, or by the data controller based on data collected, the creation of new data requires some processing of other data.

(iv) 'inferred data', which means data resulting from probability-based analytic processes, for example, statistical and profiling data. Like 'derived data', 'inferred data' requires a certain processing procedure and cannot be obtained directly through the act of a 'data subject's provision' or 'observation'. However, 'inferred data' is mainly generated by the processing behavior of the data controller, e.g. the portrait of the user drawn by the analysis of the information.

WP29 excluded 'derived data' and 'inferred data' from the concept of 'provided by'[72], and the reason is to prevent these kinds of data which are processed by data controllers[73] from being freely extracted by data subjects. It can be seen that WP

[70] De Hert and others (n 66) p7; Malgieri (n 66) 130; according to Case673-17 62, 'Active consent' is thus now expressly laid down in Regulation 2016/679. It should be noted in that regard that, according to recital 32 thereof, giving consent could include ticking a box when visiting an internet website. On the other hand, that recital expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.

[71] Drexl, J. "Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation (BEUC)"(2018) Brussels: BEUC. p108-109.

[72] WP art.242 p10. Also recommended by the EDPS, OJ C 301/1 p8, fn 34.

[73] The provider of the service or product could be regard as the data controller of the online platform.

respects the intellectual effort that the data controllers make when processing the data.

It is worth noting that the new data generated through the processing of other data does not satisfy the requirements for intellectual property rights and SGDR protection, as the data itself is not the subject of these protections. Furthermore, intellectual effort or other kinds of investment in the creation of new data through the processing of other data is also excluded from SGDR protection, due to the distinction made by the CJEU between 'created data' and 'obtained data'.

In summary, 'provided data' and 'observed data' are currently considered to be applicable to RtDP, while 'derived data' and 'inferred data' are excluded from the use of RtDP but do not fall within the scope of SGDR protection either. As the Commission stated, "like technology, the way our personal data is used and shared in our society is changing all the time and our challenge is to establish a legislative framework that will stand the test of time".[74] So with the increasing attention to the rights of data subjects, the intersection between RtDP and SGDR might cause a visible impact on the latter two kinds of data in the future.

2.3.4. The Exception of Rights and Freedoms of Others

Art. 20(4) GDPR provides for exceptions to the application of the RtDP, which means the application of the RtDP shall not adversely affect the rights and freedoms of others.[75] Although Art. 20(4) only refers to paragraph 1 (indirect portability), and paragraph 2 (direct portability) is for the purpose of paragraph 1. Art. 20(4) should also apply in the case of direct portability. However, it remains unclear as to the exact meanings of 'other' and the scope of 'rights and freedoms'.

Firstly, as the term 'other' covers both natural and legal persons. When the data

[74] COM(2010) 609 final (n 17) 18.
[75] Art. 20(4) GDPR,'The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.'

controller is presented as a legal person, it can certainly invoke this provision to refuse the data subject's request to transfer the data and thus protect its rights and freedoms. This may result in data controllers having excessive power to the detriment of the RtDP.[76]

With regard to 'rights and freedoms', there is no clear provision explaining the rights and freedoms in relation to the RtDP. But in reference to the right of access, the Recital 63 GDPR determines that it includes trade secrets or intellectual property. Considering RtDP's legislative history, which created a close relationship with the right of access.[77] Thus WP29 also stated that 'rights and freedoms' can be understood as 'including trade secrets or intellectual property', WP29 even suggested that though these rights should be considered before answering a request for data portability, "the result of those considerations should not be a refusal to provide all information to the data subject".[78]

The ambiguity of definitions have led to a significant intersection between the RtDP and other rights, in particular with the Sui Generis Database Right.

2.4 Summary

The RtDP aims to give data subjects greater control over their personal data and to facilitate data sharing. However, RtDP has encountered difficulties in application in practice, the main reasons are that i) the classification of personal data has lagged behind the reality since the emergence of connected devices; and ii) the restrictions on RtDP are not clear, creating intersections with SGDR.

[76] Drexl, (n 70) p84-5.
[77] Graef, Husovec and Purtova (n 4) p10.
[78] WP art.242. p12.

3. The relations between Personal Data and Sui Generis Database Right

3.1 Introduction

This chapter will go through a description of EU Database Directive 96/9 and SGDR. From section 3.3 onwards, the intersection of data portability and database protection will be described and analyzed.

3.2 The EU Database Directive 96/9

3.2.1 The brief introduction of EU Database Directive

The Recital 38 of Database Directive 96/9 explains the reason for database protection, as "whereas the increasing use of digital recording technology exposes the database maker to the risk that the contents of his database may be copied and rearranged electronically, without his authorization, to produce a database of identical content which, however, does not infringe any copyright in the arrangement of his database".

In the view of the Community legislator, unprotected content is at risk of reproduction and electronicisation through the creation of so-called parasitic products and services.[79] And there are significant disparities in the level of investment and legal protection of databases within the EU, especially when

[79] Nicolae Titulescu University Publishing House, "DATABASES AND THE SUI-GENERIS RIGHT-PROTECTION OUTSIDE THE ORIGINALITY. THE DISREGARD OF THE PUBLIC DOMAIN" https://doaj.org/article/221c73070bd44d3d9715e34ef5a31579, last accessed 10 may 2022.

compared to the US.[80]

Presumably, the modern market for information storage and processing systems will need protection against misappropriation to reach its full value.[81] So the Directive was worded quite broadly and is technically neutral, to provide legal protection for any type of database.[82] The legislator aimed at providing 'a wide scope, unencumbered by considerations of a formal, technical or material nature'.[83] And it also introduced a new rights protection, SGDR, in Art. 7, to incentivise investment in EU database production.[84]

3.2.2 The Concept of 'Database'

According to EU Database Directive 96/9, there are three conditions that need to be fulfilled to become a 'database': (i) it shall mean a collection of independent works; (ii) the data or other materials arranged in a systematic or methodical way; (iii) the data and other materials are individually accessible by electronic or other means.[85]

The first condition focuses on the requirement that the contents of a database are 'independent elements' , for example, works (in the sense of intellectual property law), data or other material. To avoid overlap between SGDR and copyright law, the CJEU held the view that, "independent means an autonomous informative value of the elements, i.e. when separated from the collection, their contents' value must not be affected".[86] Because copyright protects the intellectual work of the author in selecting and arranging these elements to form a new work, thus the

[80] rec 11 Directive 96/9/ EC.
[81] rec 12 and rec 39 Directive 96/9/ EC.
[82] European Commission, Directorate-General for Communications Networks, Content and Technology, Karanikolova, K., Chicot, J., Gkogka, A., et al., Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases : final report, Publications Office (2018) p4, https://data.europa.eu/doi/10.2759/04895.
[83] Case C-444/02 Fixtures Marketing [2004] ECLI:EU:C:2004:697 para 20.
[84] rec 12 Directive 96/9/ EC.
[85] Article 1(2) Directive 96/9/ EC,' For the purposes of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.'
[86] ' materials which are separable from one another without their informative, literary, artistic, musical or other value being affected' Case C-444/02 Fixtures Marketing [2004] ECLI:EU:C:2004:697.

new work has to be considered as a whole. A literary work, a musical composition or a sound recording can not be regarded as a database, even if it can be conceived as a collection of moving images, words, notes or sounds.[87] But there is no limitation on the number of elements that constitute the database.

The form of 'collection' should be understood to include both dynamic and static, on the basis that the investment in 'verification' is included in the SGDR. Verification of the data entering into a database is especially needed where circumstances on which the database seeks to inform will change over time. Although there are doubts raised on the expression in Art. 10 (1), as 'completion of the making of the database' means stability. The wording of Art. 10 (3) proves that dynamic databases are conceivable, as it allows the database right to be revived with every 'substantial change'.[88] The notion of 'completion of the making of the database' is intended only for determining the starting point of database protection.[89] To be more specific, in the German Autobahnmaut case, where the the defendant provided the lorry operator with a daily update of the cost of using the motorway, the Federal Supreme Court not only did not doubt the dynamic nature of the data, but qualified the daily transmission of the data to its partners as an independent database.

For the arrangement of data and material within the database. The Database Directive 96/9 only requires that it be presented in a 'a systematic or methodical way' but 'it is not necessary for those materials to have been physically stored in an organized manner'.[90] The third criterion of individual accessibility is related to the arrangement requirement. As long as there is a technical or other ways (such

---

[87] Rec 17 Directive 96/9/ EC.

[88] art. 10 (3) Directive 96/9/ EC, " Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection."

[89] Drexl, (n 70) p74-76.

[90] Recital 21 Directive 96/9/ EC.

as a database management software) enabling the data retrieval from an unorganized collection (such as a hard drive), the requirements are met.[91]

In summary, despite these requirements, the database remains an overly broad and open-ended concept, and depending on the case law of different countries. As SGDR has been granted for telephone directories, collections of legal materials, real estate information websites and so on.

3.2.3 The Sui Generis Database Right

(a) Requirements of Protection

According to Art. 7(1) Database Directive 96/9, SGDR protects substantial quantitative and/or qualitative investments in the obtaining, verification or presentation of database content investment.[92]

(a.i) Substantial Investment

As a neighbouring right, unlike traditional intellectual property rights which protect the intellectual works of human beings, SGDR protects the investment of the maker of the database. SGDR protects the 'sweat of the brow' of the database producer.[93] Investment in a database must be substantial, either in a qualitative or a quantitative sense. This means that in the forms of the investment, it can be qualitative investment, such as monetary or other financial means, otherwise it can be quantitative investment, such as labour, time or technological efforts.

However, for volume restriction, there is no established threshold for the number of 'substantial investments'. Although 'substantial' is defined differently by

[91] Fixtures Marketing, (n 85) para 30.
[92] Article 7(1) Directive 96/9/ EC,'Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.'
[93] Hugenholtz, P. Bernt,"Something Completely Different: Europe's Sui Generis Database Right." (2016).

national courts, it generally requires only a low level of investment.[94]

(a.ii) Investment in Obtaining, Verifying or Presenting

Further, not all investments in databases are protected by SGDR. Only substantial investments in three specific areas - (i) obtaining, (ii) verifying, or (iii) presenting the content of a database - could qualify under protection. However, there is no requirement to invest in all three of these areas at the same time, which means that investments in any of the three areas can be protected by the SGDR as long as they meet all the requirements of the SGDR.[95]

The most controversial term was 'obtaining', particularly whether investments made by database makers in creating data can be protected by SGDR and whether data generated by users through the use of data collection products[96] is data created or collected by database makers.

The question of whether investments used to create data can be protected by the SGDR has been answered by the CJEU in two cases, British Horseracing and Fixtures Marketing.[97] In these two cases, the CJEU made a clear distinction between creating elements and collecting elements, and stated that according to SGDR's purpose to promote and protect investment, the expression 'investment in ... the obtaining ... of the contents' of a database must be understood to refer to the resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent materials.[98] Therefore, only the resources used to seek out existing independent

---

[94] Annemarie C Beunen, "Protection for databases: the European Database Directive and its effects in the Netherlands, France and the United Kingdom" (2007) Wolf Legal, p138; Mark J Davison and P Bernt Hugenholtz,"Football Fixtures, Horseraces and Spin-Offs: the ECJ Domesticates the Database Right"(2005) 27 (3) EIPR, p113, 116; Estelle Derclaye, "The legal protection of databases: a comparative analysis" (2008) Edward Elgar 362, p75.

[95] Article 7(1) Directive 96/9/ EC.

[96] The data collection products, for example, body sensor and the tolling system in the Autobahnmaut case.And the data generated from the data collected by these sensors or other types of machines is generally called "machine-generated data". Beunen (n 93) p126.

[97] Case C-203/02 British Horseracing Board [2004] ECLI:EU:C:2004:695 (BHB) para31; Fixtures Marketing (n 85) para 40.

[98] British Horseracing Board case, (n 96) para 31.

materials and collect them in the database can be protected by SGDR, the resources used to create independent materials fall outside the scope of SGDR protection. These two cases also illustrate that sole-source databases are not protected, as it is not possible to prove sole-source databases requiring substantial investment in obtaining, verifying and presenting elements.[99]

On the question of whether machine-generated data can be protected by SGDR. Although the CJEU did not yet decide on a case in this regard,[100] the Autobahnmaut case[101] illustrates that protection would be available only to such pre-existing data that is capable of being independently collected, measured or observed by a third party. In this case, a toll company used its toll collection system to collect data concerning fuel card numbers, vehicle registration numbers, toll dates and length of routes traveled were considered to be obtained.[102] According to the reasoning of the BGH, this data could have been collected independently by a third party and had not been created by the company.

With regard to 'verifying'. According to the CJEU's explanation in the Fixtures Marketing case, it means that the reliability of the data within the database is ensured, as well as monitoring the accuracy of the elements collected when the database is created or operated.[103] This also illustrates the fact that databases can be dynamic, as 'verification' includes the act of checking, correcting and updating the contents of the database.[104] However, as the investment in the creation of the data has been excluded from the protection of the SGDR as mentioned above, any investment in verification made in the creation of the data itself is also excluded.

---

[99] Ibid para 35.
[100] Matthias Leistner, "Big Data in the Digital Economy: Legal Concepts and Tools" in Lohsse S, Schulze R and Staudenmayer D (eds), "Trading Data in the Digital Economy: Legal Concepts and Tools Münster Colloquia on EU Law and the Digital Economy III" (Nomos 2017) p27, 28-9, also considers the CJEU's decision in Verlag Esterbauer as supporting the distinction.
[101] British Horseracing Board case, (n 96).
[102] Ibid para 19.
[103] Fixtures Marketing, (n 85) para 43.
[104] Hugenholtz,(n 92) p212.

Last but not least, the CJEU held the view that investment in 'presenting' refers to resources which are used to give the database the functions for processing information. For example, the acts concerning digitizing (scanning) analogue files, creating a thesaurus or designing a user interface.[105] According to the Fixtures Marketing case, it means 'those used for the systematic or methodical arrangement of the materials (…) and the organization of their individual accessibility'.[106]

(b) Ownership or Authorship

According to Art. 7(1) and Recital 41 of the Database Directive 96/9, SGDR is attributed to the database producer, i.e. 'the person who takes the initiative and bears the risk of the investment', excluding subcontractors.[107] However, the Database Directive 96/9 does not provide any indication of whether database rights may have joint ownership. With the emergence of a collaborative and innovative internet environment, co-ownership of SGDR will gradually become an issue, especially in data sharing platforms for connected devices. The reasons for this potential issue are as follows: co-ownership occurs whenever two or more persons take the initiative and bear the risk of investment in the creation of a particular database. Whereas in a data sharing platform with connected devices, where the connected devices and the data sharing platform belong to two different persons but jointly produce the same database, the investor in the connected devices takes the initiative and bears the risk for the part of the database that obtains and processes the data by investing in the devices, while the investor in the data contributing platform takes the initiative and bears the risk for the part concerning the verification and presentation of the database.

Although there are situations where none of the parties realize that the resulting

[105] Ibid p211.
[106] Fixtures Marketing, (n 85) para 43.
[107] Recital 41 Directive 96/9/EC, 'whereas the maker of a database is the person who takes the initiative and the risk of investing; whereas this excludes subcontractors in particular from the definition of maker'

database will be jointly owned[108], it is more difficult for a third party to know exactly who the database maker is if there is already a problem in determining who made the database and who owns it.

(c) Scope of Protection

According to the Art. 7(1) of the Database Directive 96/9, SGDR grants database makers the exclusive rights to (i) extract and (ii) reuse 'the whole content of that database or a substantial part of it evaluated in terms of quality and/or quantity'. The SGDR is calculated from the date of completion of the database, in accordance with Art. 10, and the right lasts for 15 years following the date of completion of the database.

According to the Art. 7(2)(a), 'extraction' means 'the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form'. The CJEU also had interpreted the term 'extraction' broadly. In the Directmedia Publishing case, it can be seen that 'extraction' includes 'any unauthorized act of appropriation of the whole or a part of the contents of a database'.[109] This means that infringement is not limited to technical reproduction, by any means, including by hand. It is sufficient that the elements are consulted and copied from the database to constitute an infringing extraction as described in Art. 7.

It is worth noting that SGDR only protects substantial investments in specific four categories of behaviors, and the protection does not extend to the element in the database itself. So if another database maker obtains elements from other sources than the relevant database and creates a new database independently, then the maker of the relevant database is not able to claim exclusivity on the grounds that the elements in the database are the same.[110]

---

[108] Leistner, (n 99) p35-36.
[109] Case C-304/07 Directmedia Publishing [2008] ECLI:EU:C:2008:552 para 34.
[110] Derclaye, (n 93) 0107; Leistner, (n 99) p431.

According to the Art. 7(2)(b), 're-utilization' means 'any form of making available to the public all or a substantial part of the contents of a database, by renting, by on-line or other forms of transmission'. The term has also been interpreted extensively by the CJEU through the British Horseracing case, it refers 'to any act of appropriating and making available to the public, without the consent of the maker of the database'.[111] While according to case law, the 'public' means an indeterminate number of potential recipients and implies, moreover, a fairly large number of persons.[112]

According to the interpretation in the British Horseracing case, it is only necessary to consider the impact of the objective act when examining the infringement, regardless of the purpose of the extraction and/or re-utilization.[113] This means that whether the extraction and/or re-utilization is for the purpose of creating a new database or for other activities is irrelevant. It is sufficient that the act of extraction and/or re-utilization of all or a substantial part of the contents involves the manufacture of a parasitic competitive product, or other acts that would cause substantial damage (quantitatively or qualitatively) to the investment in the database.[114] It is worth mentioning that, in evaluating whether the impact of the extraction and/or re-utilization is significant, damage to the database producer's substantial investment in obtaining, verification or presentation of the content shall be considered solely. Rather, the intrinsic economic value of the affected elements themselves is not the subject of assessment.

When assessing whether the damage to an investment has reached a substantial

---

[111] British Horseracing Board case, (n 96) para 51.

[112] Judgments of 15 March 2012, SCF, C-135/10, EU:C:2012:140, paragraph 84; of 31 May 2016, Reha Training, C-117/15, EU:C:2016:379, paragraph 41, and of 29 November 2017, VCAST, C-265/16, EU:C:2017:913, paragraph 45 and the case-law cited.

[113] Estelle Derclaye, (n 93) p119.

[114] Recital 42 Directive 96/9'the right to prohibit extraction and/or re-utilisation of all or a substantial part of the contents relates not only to the manufacture of a parasitical competing product but also to any user who, through his acts, causes significant detriment, evaluated qualitatively or quantitatively, to the investment'; British Horseracing Board case, (n 96), para 47.

level, it can be assessed in both quantitative and qualitative terms. In quantitative terms, the substantial part refers to the volume of elements extracted or re-utilized from the database in relation to the volume of the database's contents as a whole.[115] So this volume needs to be analyzed case by case. And It is irrelevant whether this part of the content is constituted as the substantial content of another database.[116]

The assessment of the qualitatively substantial focus on the scale of the investment made by the original database maker in the obtaining, verification or presentation of the relevant database element. And this is irrelevant whether the relevant database elements constitute a quantitatively substantial part.[117] As mentioned above, investments can be in money, time and labour, etc.

Moreover, Art. 7(5) of the Database Directive 96/9 limits the repeated and systematic extraction and/or re-utilization of non-substantial parts by two exceptions -- if they (i) intersect with a normal exploitation of the database, or (ii) unreasonably prejudice the legitimate interests of the database maker.[118] The main purpose of this provision is to prevent the multiple, repeated and systematic extraction of non-substantive parts that gradually result in the reconstruction of the database as a whole or of a substantial part. The scope of the SGDR was further extended through the British Horseracing case, in which the CJEU held that exhaustion after the first sale of a copy under Art. 7(2)(b) of the Database Directive 96/9 applies only to the right to resell that copy, so that extraction and re-utilization based on a copy of a third party's database is also an infringing act.[119]

---

[115] British Horseracing Board case, (n 96) , para 70.
[116] Beunen (n 93) p186; Derclaye (n 93) p110.
[117] British Horseracing Board case, (n 96) , para 71.
[118] art. 7(5) Directive 96/9, 'The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted.'
[119] Davison and Hugenholtz (n 93) p117.

(d) Exceptions and Limitations

Art. 9 of Database Directive 96/9 lists three exceptions: (i) private purposes regarding non-electronic databases; (ii) illustration of non-commercial teaching or scientific research; and (iii) public security or administrative or judicial procedures. The first two include only extraction, while the latter refers to both extraction and re-use. In addition, the exception covers only extraction and/or re-utilization of a substantial part (not the whole) of the content of a database, which is made available to the public by the maker.

3.3 Connections between the Right to Data Portability and the Sui Generis Database Right

As discussed in Chapter 2, the effects of RtDP include strengthening the individual's right to control data and breaking the 'lock-in effect' of data, but as the GDPR does not exclude the application of RtDP to data in databases. Therefore, when data subjects are free to transfer personal data acquired by database producers through extraction and re-utilization, this is likely to violate the exclusive rights granted to database makers by the SGDR. Meanwhile, despite the fact that SGDR does not protect the elements in the database, the database maker may not need a substantial investment in acquiring the elements in the database in order to obtain the data. Especially when the data elements can be easily transferred. It is reasonable to assume that the rationale for SGDR to protect the investments of database makers will be challenged.

3.3.1 The Controller of Data and The Owner of Database

There is no doubt that the information in a database can contain personal data, then an online database that functions to collect and process personal data can also be considered as a database under certain conditions.

This chapter divides the data into those obtained directly by the online platform

and those obtained indirectly by connecting the device to the online platform, in terms of direct and indirect access to the data.

(a) Online Platforms

When the content of an online platform consists of personal data, such online platforms are likely to be classified as databases,[120] and the database in this case generally contains the personal data of several users. While each user's individual online platform account may also become a database, in which case the database contains only the data collection of a specific data subject.

In the first place, most of the content created and posted by users of online platforms can be related to an identified or identifiable natural person, such as photos, comments, emails, browsing history and location data. So this kind of content meets the identifiability requirement, and can be defined as 'personal data'. And data subjects of the online platform, i.e. users, should be able to enjoy the rights granted by the RtDP.

Some personal data in online platforms are knowingly and voluntarily provided by users, such as comments and photos. Although there is a debate about this type of data 'as it is created in real time rather than pre-existing data'[121], the CJEU's distinction between 'obtaining' and 'creating' is limited to elements created by the database maker and does not concern elements created by third parties. There is therefore no reason to exclude the data created by the user in real time and accessed by the database maker from the scope of protection of the Database Directive 96/9. There is also some data obtained based on the pre-existing data, such as users' preferences, movement traces. This can be argued that the data was created rather than obtained by the database makers. This kind of data, which

[120] Graef, Essential Facility (n 4) p142.

[121] Graef, Essential Facility (n 4) p142-143 also argues that from the obtaining-creating distinction, online platforms could have an issue in claiming Database Right on data that is inferred from the user's use of the platform. However, considering that inferred data is generally not considered data 'provided by the data subject' under the RtDP, it is not of an issue for the specific analysis of this research.

needs to be based on the user's previously used and created data behavior, runs the risk of falling outside the scope of RtDP. And this is more frequently happening on online platforms with connected devices, which will be explained in more detail in later sections.

In second place. According to the GDPR, the operator of an online platform is a data controller as the operator decides, alone or jointly with others, the purposes and means of processing personal data. And personal data in online platforms require significant resources to set up such platforms to collect personal data from users, keep them updated and monitor the accuracy of the collected elements.[122]

In addition, most online platforms have the function of information retrieval[123], which demands that the makers of online platforms present data in the way specified in SGDR.[124] In the case of Instagram, for example, a user's photo can be presented in a personal account with different tags, appearing in both story and highlight, or a user's name can be searched to find different friends with the same name and browse their home pages.

Therefore, it can be seen that the initiative and risk of investment in obtaining, verification and presentation will usually be taken by the online platform operator, i.e. the database maker, i.e. the data controller. For this reason, the online platform has the potential to be protected by SGDR.

In conclusion, it can be observed that according to Database Directive 96/9, an online platform consisting of personal data may become a database, which leads to the intersection of SGDR and RtDP.

---

[122] Ibid p481.
[123] Ibid p142.
[124] The CJEU held the view that investment in 'presenting' refers to resources which are used to give the database the functions for processing information. According to the Fixtures Marketing case, it means 'those used for the systematic or methodical arrangement of the materials (…) and the organization of their individual accessibility'. The requirement for 'presentation' can therefore be considered as enabling database data processing functions.

(b) Connected Devices

Because of the increasingly widespread use of connected devices, there are some difficulties in defining personal data. It is not clear whether the manufacturer of the connected device is the controller of the online platform (database maker) to which it is connected or another third party, depending on how the personal data is processed. But the connected devices are usually linked to some service provision or online platform,where individuals provide additional personal data.[125] All data obtained by connected devices, including personal data, will most frequently be structured in databases.[126] In this circumstance, a controversy arose as to who the SGDR should be granted to, when the controller of the connected device and the controller of the online platform are not the same subject.[127] It is undeniable that the user who purchases or uses the connected device also makes an investment and takes the risk of collecting its data. Unfortunately, however, the user's investment is usually in the creation of data, which cannot be protected by SGDR. And given the 'initiative' requirement, the SGDR will usually be granted to the manufacturer of the connected device.[128] So it comes back to the question of who the manufacturer of the connected device is and who the SGDR should be granted to.

Data generated and obtained by the database maker through connected devices has its unique characteristics. As data generated by a user through the use of a product(connected devices), like data generated by a user through the use of a service, is subject to the user's usage behavior to make it available to the database producer and to be obtained in the database. It is also worth noting that users may not be aware that their data is being collected when they are using and generating data by using a product or service, which departs from the RtDP requirement that 'the data is provided by the data subject', and that data generated by users during

[125] Elfering, Stephanie, (n 5) p45
[126] Herbert Zech, "A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data" (2016) 11 (6) JIPLP, p468.
[127] Elfering, Stephanie, (n 5) p47-49
[128] Drexl, (n 70) p77; Leistner, (n 99) p37.

their use of products or services may be based on other data. This could lead to this type of personal data, which needs to be used by the user in order to be generated and obtained, falling within the scope of 'observed data'[129] or 'derived data'[130] and being questioned on whether RtDP can be used.

3.3.2 How is the intersection between data portability and the sui generis database right

The intersections of RtDP and SGDR have been illustrated above. These intersections lie mainly in the fact that, in certain circumstances, 'personal data' in the RtDP overlaps with data in databases and online platforms that can be considered as databases and protected by the SGDR. The maker of the database, in turn, enjoys the exclusive rights granted by the SGDR while at the same time fulfilling the obligations imposed on it by the RtDP as a data controller. And where the data controller fulfills its obligations in accordance with the rights conferred on the data subject by the RtDP, the most relevant part of its own rights is that the transfer of data involves 'extraction' and 're-utilization'.

In the case of phone number portability, for example, even if the data subjects themselves have no initiative to port their data, data controllers on other online platforms might be very willing to persuade data subjects to make the portability request by offering discounts and other offers. While the extracted content may be substantial in relation to the whole (including where the sum of a single or multiple extractions by a data subject add up to an extraction of the substantial content of the database; and where the extractions by multiple data subjects together result in an infringement of the substantial content of the database). Consequently, a portability request could potentially be understood as an unlawful extraction.

---

[129] 'observed data', which are observed from the individual and recorded by a third party, for example, sensors such as smart wearables used for mobile health care, checking the bodily functions of a patient.
[130] 'derived data', which means new data generated based on other data from the individual, for example, computational and notational data.

Moreover, with the support of online transmission technology, data obtained by means of direct or indirect portability can be easily available to the public by both data subjects and data controllers. The database maker's exclusive right to prevent the re-utilization of substantial parts of the content of his database might also be infringed. As whenever personal data extracted on the basis of the RtDP is made available to an indeterminate number of people, this constitutes 'making available to the public'. And the condition of making it available to an indeterminate number of people is extremely easy to fulfil in the Internet age, for example by posting it on an online platform.

In addition, based on the interpretation of the scope of protection of the SGDR, in the case of extraction or re-utilization of insignificant parts, these acts may also be infringements if they are repeated and systematic.

3.4 Summary

In situations where online platforms and connected devices are present. The subject and the object of the SGDR, the database maker, the data and the database, have the potential to overlap with the data controller, personal data and online platform in the RtDP.

When users of an online platform use data portability rights as data subjects, it is also difficult to avoid the extraction and re-utilization of the content of the online platform's database. This can be regarded as the intersection of the data subject's right to data portability and the database maker's exclusive right to prevent others from illegally extracting and reusing the database content.

Consequently, it is worth doubting whether database makers need to invest substantially on obtaining data in an environment where data sharing is so convenient.

4. The Potential Impact of Art.35 in EU Data Act

4.1 Introduction

This chapter will focus on the proposed Art. 35 in EU Data Act. The first part will provide an introduction to the proposed EU Data Act. The second part will address why Art.35 is relevant to data portability and database protection. The third part of the chapter will discuss the possible scope of application of Art.35 through case studies, i.e. answering the question of what is meant by 'data obtained from or generated by the use of a product or a related service'. In the fourth part, the potential impact of Art. 35 in the proposed EU Data Act on RtDP and SGDR is discussed.

4.2 The background of Art.35 in EU Data Act

4.2.1 The EU Data Act

The release of the proposed EU Data Act on 23 February 2022 indicates a greater attention to the value of data in the digital economy, as well as to the control of data, which seems to reflect a legislative initiative to increase trust and facilitate the sharing of data across the EU and between sectors.[131]

Although the proposed EU Data Act will not set any new rights or amend existing rights on access to and use of data, it is complementary to the Data Governance Act. The Data Act will lay down harmonized rules on: (i) making data generated

[131] "On 23 February 2022, the European Commission presented its Proposal for a Data Act, a Regulation aimed at maximizing the value of data in the European Union economy 'by ensuring that a wide range of stakeholders gain control over their data and that more data is available for innovative use.'"The Platform Law Blog, "The EU Data Act – the Commission's latest legislative initiative" (2022) https://theplatformlaw.blog/2022/02/25/the-eu-data-act-the-commissions-latest-legislative-initiative/?blogsub=confirming#subscribe-blog. Last accessed 25th May 2022.

by the use of connected products or related services available to the user of these products or services; (ii) making data available by data holders to data recipients; and (iii) making data available by data holders to public sector bodies or EU institutions, agencies or bodies in cases of exceptional need. And The most relevant to the study of this paper is the forthcoming work on the first purpose. So the following discussion of the proposed EU Data Act will therefore focus mainly on the proposed articles relating to the first purpose.

The core objective of the EU Data Act is placing users and service providers on a more equal footing in terms of access to data. Specifically, the EU Data Act aims to make more data available for use, it wants everyone to have access to data they have contributed in its generation.[132] The Data Act will include various obligations for different categories of data stakeholders, which includes (i) manufacturers of connected products or related services (that is, services incorporated in or inter-connected with a connected product in such a way that their absence would prevent the product from performing one of its functions); (ii) data holders (defined broadly as legal or natural persons having the right or obligation, in accordance with the Data Act, applicable EU law or national legislation implementing EU law to make available certain data), and (iii) cloud and edge service providers.[133]

Chapter II of the EU Data Act focuses on the rules for manufacturers of connected products and related services. It sets out rights and obligations regarding access to and use of data generated through the use of these products and services. In Art. 3, it imposes the obligation to design those products and services in a way that data are 'by default, easily, securely and, where relevant and appropriate, directly accessible to the user'. Furthermore, through Art.4, the proposed EU Data Act

[132] DR2 Consultants 'European Data Act: a harmonized framework for accessing and sharing data' https://dr2consultants.eu/european-data-act/.Last accessed 25th May 2022.
[133] The Platform Law Blog, "The EU Data Act – the Commission's latest legislative initiative" https://theplatformlaw.blog/2022/02/25/the-eu-data-act-the-commissions-latest-legislative-initiative/?blogsub=confirming#subscribe-blog.Last accessed 25th May 2022.

introduces a right for users to access and use data generated by their use of a connected product or service, as well as a right for third parties to access such data upon the user's request (Art.5). According to these articles, the scope of application of the data subject's indirect portability right (Art.4) and direct portability right (Art.5) might be extended.

From the expression "In order not to hinder the exercise of the right of users to access and use such data in accordance with Art.4 of this Regulation or of the right to share such data with third parties in accordance with Art.5 of this Regulation" in Chapter 5 Art.35. It is clear that the purpose of Art.35 is to ensure that these rights can be used on 'certain data'[134]. What is more, Art.35 is devoted to the explanation of databases involving 'data obtained from or generated by the use of a product or a related service'[135], and it might approve the application of RtDP to such databases.

4.2.2 The relationship between Art.35 and data portability

Although there is no explicit reference to the RtDP in the original text of Art.35, it is reasonable to assume that Art.35 will have an impact on the RtDP.

On the one hand, the proposed Data Act has the same purpose as the RtDP. As to ensure the right of data subjects to receive and transfer personal data and to facilitate data sharing. Regarding the explanatory memorandum of the EU Data Act - in response to the European Council's emphasis on interoperability and the increased demand for portability of the EU cloud[136] - it is possible to understand the aim of the Data Act to diminish wider data access and use. More obviously, the Commission and EU Member States were asked to examine actors' rights and

[134] Data generated by their use of a connected product or service.
[135] Art. 35 Databases containing certain data EU Data Act proposal 'the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.'
[136] European Council, European Council meeting (1-2 October 2020) - Conclusion EUCO 13/20, 2020, p. 5. "the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as interoperability"

their obligations to access data they have been involved in generating and to improve their awareness of, in particular, the right to access data and to port it.[137]

On the other hand, if the data involved in Art.4 and Art.5 meet the three conditions of the RtDP, the right of portability can certainly apply. It would be reasonable to consider Art.4 and Art.5 as complementary to the scope of data covered by the existing RtDP. Although only the SGDR is mentioned in the Art. 35 without any explicit reference to the RtDP, the Art. 35 may still clarify the role of the SGDR and RtDR.

4.2.3 The relationship between Art.35 and Sui Generis Database Right

Art. 35 makes it clear that any data obtained from or generated by the use of a product or a related service is not protected by SGDR. While the recital 84 explains that "this Regulation should clarify that the sui generis right does not apply to such databases as the requirements for protection would not be fulfilled". There is no doubt that Art. 35 might free certain type of data from the sui generis database protection.

However, some arguments have been made that removal of certain type of data from database protection will not affect SGDR. The reason is that in the British Horseracing case, the CJEU clearly stated that "investment in ... the obtaining ... of the contents' of a database in Art. 7(1) of the directive must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database."[138]

---

[137] EU Data Act, p3 'As such, the Commission and EU Member States were asked to examine actors' rights and their obligations to access data they have been involved in generating and to improve their awareness of, in particular, the right to access data, to port it, to urge another party to stop using it, or to rectify or delete it, while also identifying the holders and delineating the nature of such rights.'

[138] British Horseracing Board case, (n 96).

To be specific, firstly, the resources used to seek out existing independent materials and collect them into the database refer to the resources used to create the product and related service, which can be protected by SGDR.

Secondly, the data that constitutes the material of the database is generated through the user's use of the product and related service. Although, during the use of product and related service, users might put the investment in the creation of the database material, the investment in the creation of the data cannot be protected by the SGDR under the interpretation of this case.

Thirdly, it is undisputed that the data generated through the use of the user cannot be protected by the SGDR.

Although, based on these three points, Art.35 can be understood as having no effect on SGDR. However, if data subjects are free to transfer the personal data, database makers might not need to invest substantially in the resources for obtaining existing material and collecting it in the database, i.e. for 'creating products and related services'. This would make the investment in this field not meet the 'substantial' requirement in Art. 7(1) Database Directive.

Furthermore, according to the interpretation of the database in Fixtures Marketing. When another data controller accepts data transferred from a previous database by a data subject, it is only necessary to satisfy the 'the materials are individually accessible' and 'the materials are arranged in a systematic or methodical way'.[139] And then the materials transferred can also constituted a database in the sense of the Database Directive. Even this acknowledges the latter database maker's investment in verification and presentation, it is clearly disrespectful of the former database maker's investment in obtaining data.

[139] Fixtures Marketing (n 85) .

4.3 What is ‘data obtained from or generated by the use of a product or a related service’

Following the analysis of the background of the EU Data Act in previous chapter, according to the obligation subjects it will affect, the products and services in question must have a direct connection with the online platform[140]； At the same time, since the proposed EU Data Act consistently continues the purpose of the Data Governance Act to facilitate voluntary data sharing, and might be an extension of the RtDP in the GDPR. The ‘data obtained from or generated by the use of a product or a related service’ also needs to meet the requirements of ‘relate to an identified or identifiable data subject’ and ‘provided by the data subject’ in order to meet RtDP’s requirements and delineate the boundary of right.

4.3.1 Analysis

The product and related services must have a direct connection to the online platform. More specifically, without this related product or service, the online platform would not be able to perform a particular function.

A direct connection does not mean that the product or related service in question has to be embedded in an online platform. Examples of formal separation from the online platform are wearable connected devices such as sports watches, which often work with an online data analysis platform to implement data analysis functions. The device acts as a data collector for various body indicators and transmits the data obtained to an online platform. The online platform analyses the data such as heart rate, respiratory rate, length of exercise, etc. to produce a comprehensive analysis of the calories consumed, which is referred to as ‘data

[140] “The Data Act will include various obligations for different categories of data stakeholders, which includes (i) manufacturers of connected products or related services (that is, services incorporated in or inter-connected with a connected product in such a way that their absence would prevent the product from performing one of its functions)”The Platform Law Blog, “The EU Data Act – the Commission’s latest legislative initiative” (2022) https://theplatformlaw.blog/2022/02/25/the-eu-data-act-the-commissions-latest-legislative-initiative/?blogsub=confirming#subscribe-blog

obtained from or generated by the use of a product or a related service'.

The products and services embedded in the online platform are often reflected in the various functions provided by the online platform, such as the product browsing service and the recommendation of products according to user preferences provided by the shopping online platform. The online platform will analyse user preferences based on data generated by the use of browsing services, and the resulting user profile is known as 'data obtained from or generated by the use of a product or a related service'.

In C-345/17, as the users of the online platform are using their own devices -- digital photo cameras -- to generate videos. This digital photo camera is independent of the online platform and is not directly linked to it, and whether it exists or not does not affect the function of sharing videos on this online platform.[141] Thus, even the user generated personal data, i.e. a video, using this digital photo camera, and the video falls within the scope of the RtDP in this case without doubt, it is not 'data obtained from or generated by the use of a product or a related service'.

The requirements of 'relating to an identified or identifiable data subject' and 'provided by the data subject' should be met.

For the requirement of 'provide by data subject'. When the user, i.e. the data subject, uses a connected device, the data subject is in fact actively and knowingly generating the data himself, as well as when using the relevant service. Furthermore, if the user is unaware of the fact that he or she is generating data in the course of using the product or service, he or she will not wish to exercise the rights granted to them in the proposed EU Data Act to transfer the data.

[141] Case C-345/17 Buivids [2019] ECLI:EU:C:2019:122

For the requirement to ‘relate to an identified or identifiable data subject’. C-582/14 lists some of the data generated by users through the use of several websites operated by German federal agencies, such as the terms entered in the search fields and the quantity of data transferred.[142] However, the CJEU held that some of this data could not fall under the protection of the GDPR because it cannot identify the user. This means that ‘data obtained from or generated by the use of a product or a related service’ needs to meet the requirement of being identifiable to the user.

4.3.2 Examples

While carrying out a case search, four cases listing examples of ‘data obtained from or generated by the use of a product or a related service’ come to the attention. And although none of the disputes in these cases were related to data classification, I find they would be beneficial to include in my thesis to help me explain the question concept.

i) C-40/17 Fashion ID. Fashion ID, as the operator of a website, allows Facebook to embed a plug-in on that website that collects personal data, namely the Facebook ‘Like’ button. when a user visits Fashion ID’s website, that user’s personal data, i.e. preferences, are transmitted to Facebook. [143]In this case the user generated data about the user’s preferences through the use of Fashion ID, then Fashion ID can be considered a product or a related service and the data about the user’s preferences displayed on the Facebook page can be considered ‘data obtained from or generated by the use of a product or a related service’.

ii) C-673/17 Planet49. Planet49 is a lottery organizer and when a user wishes to enter a lottery they will receive a checkbox containing a checkbox containing a preselected tick (‘the second checkbox’) read: “I agree to the web analytics service Remintrex being used for me. This has the consequence that, following

[142] Case C-582/14 Breyer [2016] ECLI:EU:C:2016:779
[143] Case C-40/17 Fashion ID [2019] ECLI:EU:C:2019:629

registration for the lottery, the lottery organizer, [Planet49], sets cookies, which enables Planet49 to evaluate my surfing and use behavior on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests....".[144] Thus Planet49 is a product or a related service, and the data generated when browsing is 'data generated by using a related service'.

iii) C-319/20 meta platform Iraland. Facebook an area called 'App-Zentrum' ('App Center') on which Meta Platforms Ireland makes available to users free games provided by third parties. When consulting the App Center of some of those games, an indication appears informing the user that the use of the application concerned enables the gaming company to obtain a certain amount of personal data and, by that use, permission is given for it to publish data on behalf of that user, such as his or her score and other information. In addition, in the case of a specific game, it is stated that the application has permission to post the status, photos and other information on behalf of that user. [145]Therefore, the game is product or a related service， while the game score, the status, photos and other information on behalf of that user are 'data generated by using related service'.

iv) C-301/06- Irlande / Parlement et Conseil. It is worth noting that, in this case, Art. 3(1) of Directive 2006/24 contained expressions similar to 'data obtained from or generated by the use of a product or a related service', which is "...those data are generated or processed by providers of ... communications services or ... in the process of supplying the communications services concerned".[146] In addition, the wording of Art. 3 (1) implies that the data categories listed in Art.5 of Directive 2006/24 are likely to be generated or processed by providers of electronic communications services or public communications networks in the course of providing the communications services in question. And the data categories described in Art.5 are as follow:

---

[144] Case C-673/17 Planet49 [2019] ECLI:EU:C:2019:801

[145] Case C-319/20 Meta Platform Iraland [2022] ECLI:EU:C:2022:322

[146] Art. 3(1) of Directive 2006/24 'By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Art.5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.'

(a) data necessary to trace and identify the source of a communication;

(b) data necessary to identify the destination of a communication;

(c) data necessary to identify the date, time and duration of a communication;

(d) data necessary to identify the type of communication;

(e) data necessary to identify users' communication equipment or what purports to be their equipment;

(f) data necessary to identify the location of mobile communication equipment

4.4 The potential impact of Art.35 in EU Data Act

4.4.1 The potential impact on Right to Data Portability

On the one hand,, Art.35 is undoubtedly a proposal that will benefit the RtDP. As this thesis classifies and explains for personal data in Chapter 2, 'provided data' 'observed data' and 'derived data' may all contain large contributions from users, or exclude the possibility of sole contributions from data controllers. In line with the EU Data Act's desire to give everyone that contributes to the generation of data the legal right to access data, the types of personal data that RtDP can cover may be extended to 'derived data'. And this will contribute that users will get standard access to the generated data on any of their integrated tools (virtual assistants, connected home appliances). This means facilitating data sharing on a wider range of data, which is reflected in two ways: (i) the data could be easily and freely accessible and shareable with third parties, (ii) better access to data collected or produced by a device.

On the other hand, however, the proposed legislation mandates data sharing requirements, the European Commission has opted for a one-size-fits-all solution that compels almost all businesses to adapt, only SMEs are exempted from these obligations. Neither data holders nor third parties will be allowed to influence or prevent the user's data sharing behavior in any coercive, manipulative or technical way. Only micro and small companies will be excluded from these strict

guidelines if they are independent from other companies.

The expansion of the scope of RtDP might also exacerbate its relationship with some of the problems that already existed.

As it is more urgent to put in place certain limits to ensure that third party access to shared data is secure and harmless to all parties concerned, thereby limiting the use of data by market competitors of the data holder. Since a greater scope of RtDP means a greater possibility of involving trade secrets, privacy, confidentiality. This also means greater requirements for interfaces and platform compatibility with all other services. In order to realistically work towards interoperability, there needs to be a degree of harmonized standards between cloud services. Last but not least, particular attention needs to be paid to the risk of non-EU countries gaining access to data. Because the proposed European data act goes beyond the current limits on the transfer of personal data outside the EU, it extends such restrictions to non-personal data, such as 'derived data' . So the relevant international agreements will become very important.

4.4.2 The potential impact on Sui Generis Database Right

EU policy makers seem to be more inclined to talk about the benefits that data can bring than the benefits that limiting data can bring. To quote the European Commission:

"The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions...[The] potential [of data] should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage."[147]

[147] Diruptive Competition Project, "How the Data Act can make Europe fit for the Digital Age"(2022) https://www.project-disco.org/european-union/090221-how-the-data-act-can-make-europe-fit-for-the-digital-age/. Last accessed 25th May 2022.

And the reality is that data is already increasingly being shared between European companies. According to a recent study by the European Commission, "around 40% of the companies surveyed reported sharing and/or reusing data with other companies". Even for companies that have not yet made this leap, the study reports that "a significant proportion [of them] expect to start sharing and reusing data within the next five years".[148]

So, it seems that strengthening the facilitation of data sharing is a logical approach for the times. But does this mean that the SGDR will be abandoned in the future? As facilitating data sharing would undermine the investment invested by the database maker in obtaining the data and would also infringe the database maker's exclusive right to prevent the extraction and re-utilization of all or a substantial part of its contents. I believe that even though the facilitation of data sharing attacks the core of SGDR, it still makes sense to use SGDR to protect the investment interests of database makers until a large number of related cases arise.

4.5 Summary

Even though Art. 35 in the EU Data Act does not explicitly state that it will have an impact on the RtDP. In combination with the context and the potential need for the proposed EU Data Act, however, it appears that Art. 35 would, in certain circumstances, bring a complement to the scope of application of the RtDP.

Art. 35 will release certain data in SGDR. This may not be disruptive to SGDR. But if the EU Data Act comes into force, more attention should be given to the intersection of SGDR and RtDP.

[148] Diruptive Competition Project, "How the Data Act can make Europe fit for the Digital Age"(2022) https://www.project-disco.org/european-union/090221-how-the-data-act-can-make-europe-fit-for-the-digital-age/. Last accessed 25th May 2022.

5. Conclusion

The intersection of SGDR and RtDP is particularly obvious in an Internet environment with online platforms and connected devices. This is mainly reflected as the potential overlap of concepts involved in SGDR and RtDP. As database maker, data and database, may also be a data controller, personal data and online platform. At the same time, data subjects' requests to receive and transfer data may constitute restricted extraction and re-utilization actions in SGDR. Last but not least, it cannot be dismissed that a more convenient transfer of data might cause database makers to invest less in obtaining data.

The wording of Art. 35 clearly shows that some certain data will be released from the SGDR. The impact on the RtDP is not explicitly worded, but through analysis of the related Art. 4 and 5, it is clear that in certain circumstances, 'data obtained from or generated by the use of a product or a related service' will be included in the scope of the application of RtDP.

The proposed scope of application of Article 35 depends on the definition of 'data obtained or generated from the use of a product or a related service'. What is known is that this certain data needs to meet three requirements: (i) The products and services that obtain or generate the certain data must have a direct connection to the online platform; (ii) The certain data has to relate to an identified or identifiable data subject; (iii) The certain data has to be provided by the data subject.

It is well recognized that the perceived need of Art.35 is to facilitate wider data

sharing. It is also clear from the perceived need of Art.35 that RtDP will benefit from it. And while the impact on SGDR remains difficult to characterize. It seems reasonable to assume that the potential negative impact of SGDR on data sharing might make SGDR undesirable in the future. With the proposed EU Data Act, more attention should be focused on the intersection of RtDP and SGDR.

Bibliography

Official Publications

COM (2015) 192.

COM (2017) 9.

COM (2010) 609.

COM(2012) 11.

European Parliament, "Report on the 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)".

European Commission, Special Eurobarometer (EB) 359, "Data Protection and Electronic Identity in the EU" (2011).

OECD, "Summary of the OECD Privacy Expert Roundtable on 21 March 2014 Protecting Privacy in a Data-driven Economy Taking Stock of Current Thinking" (2014) DSTI/ICCP/REG.

European Commission, Directorate-General for Communications Networks, Content and Technology, Karanikolova, K., Chicot, J., Gkogka, A., et al., "Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases" (2018) Publications Office.

Literature

Book:

Elfering, Stephanie, "Unlocking the Right to Data Portability: An Analysis of the Interface with the Sui Generis Database Right" 1st edition, Nomos Verlagsgesellschaft, Baden-Baden, Germany (2019).

Paul Voigt and Axel von dem Bussche, "The EU General Data Protection Regulation (GDPR): A Practical Guide" Springer (2017).

Lohsse S, Schulze R and Staudenmayer D (eds), "Trading Data in the Digital Economy: Legal Concepts and Tools" Nomos (2017)

Article:

Graef, Inge and Husovec, Martin and Purtova, Nadezhda, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" (2017). vol. 19, German Law Journal 2018, no. 6, p. 1359-1398.

Kevin Allison, "Social networks may find it does not pay to be too possesive", (2008). Financial Times.

Randal C. Picker, "Competition and Privacy in Web 2.0 and the Cloud" (2008). John M. Olin Law & Economics Working Paper.

Jasper P. Sluijs, Pierre Larouche, and Wolf Sauter, "Cloud Computing in the EU Policy sphere" (2006). TILEC Discussion Paper.

Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" (2018). Law, Innovation and Technology 10 (1).

Vanberg AD and Ünver MB, "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?"(2017) 8 (1) EJLT.

Lachlan Urquhart, Neelima Sailaja and Derek McAuley, “Realising the Right to Data Portability for the Domestic Internet of Things”. (2017)

Graef, Inge, “Data As Essential Facility : Competition and Innovation On Online Platforms”. (2016)

Gianclaudio Malgieri, “User-provided personal content in the EU: digital currency between data protection and intellectual property”(2018) 32 (1) IRLCT.

Paul De Hert, Vagelis Papakonstatinou, Gianclaudio Malgierei, Laurent Beslay and Ignacio Sanchez, “The right to data portability in the GDPR: Towards user-centric interoperability of digital services”(2018) Computer Law and Security Review.

Drexl, J. “Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation (BEUC)”(2018) Brussels: BEUC.

Hugenholtz, P. Bernt,”Something Completely Different: Europe’s Sui Generis Database Right.” (2016).

Annemarie C Beunen, “Protection for databases: the European Database Directive and its effects in the Netherlands, France and the United Kingdom” (2007) Wolf Legal.

Mark J Davison and P Bernt Hugenholtz, “Football Fixtures, Horseraces and Spin-Offs: the ECJ Domesticates the Database Right”(2005) 27 (3) EIPR.

Estelle Derclaye, “The legal protection of databases: a comparative analysis” (2008) Edward Elgar.

Herbert Zech, “A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data” (2016) 11 (6) JIPLP.

Online sources

European Commission, “Shaping Europe’s digital future” (2022). <Link:https://digital-strategy.ec.europa.eu/en/policies/data-act. Last accessed 25th May 2022>.

Nicolae Titulescu University Publishing House, “DATABASES AND THE SUI -GENERIS RIGHT - PROTECTION OUTSIDE THE ORIGINALITY. THE DISREGARD OF THE PUBLIC DOMAIN” (2018) <Link:https://doaj.org/article/221c73070bd44d3d9715e34ef5a31579. Last accessed 25th May 2022>.

The Platform Law Blog, “The EU Data Act – the Commission’s latest legislative initiative” (2022) <Link:The EU Data Act – the Commission’s latest legislative initiative – The Platform Law Blog.Last accessed 25th May 2022>.

DR2 Consultants, “European Data Act: a harmonized framework for accessing and sharing data” (2022) <Link: https://dr2consultants.eu/european-data-act/.Last accessed 25th May 2022>.

Diruptive Competition Project, “How the Data Act can make Europe fit for the Digital Age” (2022) https://www.project-disco.org/european-union/090221-how-the-data-act-can-make-europe-fit-for-the-digital-age/. Last accessed 25th May 2022.

Cases

Case C-319/20 Meta Platform Iraland [2022] ECLI:EU:C:2022:322

Case C-673/17 Planet49 [2019] ECLI:EU:C:2019:801

Case C-40/17 Fashion ID [2019] ECLI:EU:C:2019:629

Case C-582/14 Breyer [2016] ECLI:EU:C:2016:779

Case C-345/17 Buivids [2019] ECLI:EU:C:2019:122

Case C-304/07 Directmedia Publishing [2008] ECLI:EU:C:2008:55

Case C-203/02 British Horseracing Board [2004] ECLI:EU:C:2004:695

Case C-444/02 Fixtures Marketing [2004] ECLI:EU:C:2004:697

Case C-434/16 Nowak [2017] ECLI:EU:C:2017:994