Big Data and Data Protection in the Context of EU Competition Law

Janne Tarkoma
Institutionen för redovisning och handelsrätt

Hanken Svenska Handelshögskolan

Helsingfors
2018
Digitalization is changing traditional market conditions and this rapid technological development is likely to affect both economic operators, and consumers as individuals. Processing of vast quantities of digital information is an increasingly important feature of many business models in the digital economy and these data sets often include information that can be qualified as personal data within the meaning of article 4 of the General Data Protection Regulation (GDPR). Due to the increasing strategic and economic value of personal information for undertakings in the digitalized world, it is necessary to be able to ensure the compliance with EU data protection legislation. Despite the reform of European data protection framework and entry into force of the new GDPR in May 2018, it seems still relatively difficult to find a broad consensus on the balance between promotion of economic activity and an adequate level of protection of personal data in the European Union.

Although many of the digital services provided in the data-driven economy are seemingly free of charge for individual consumers, it seems clear that the collection, storage and analysis of personal data confer a substantial competitive advantage for many private entities in the digital business ecosystem. Moreover, these data related business practices are undoubtedly of a commercial nature. However, it is equally important to acknowledge the protection of personal data as a fundamental right recognized by article 8 of the Charter on Fundamental Rights of the European Union and article 16(1) TFEU. In addition, since personal data are often integrated into consumer products and services, many questions stemming from data protection law have become consumer issues. As a result of rapidly growing economic exploitation of large data sets in the digital marketplace, this informational expansion is likely to create new risks also in the context of European competition law and enforcement. The market concentration is relatively high in many of the digital sectors of economy and potential anti-competitive acts and practices may occur. Despite the somewhat flexible and adaptive nature of EU competition rules, it is not clear whether traditional competition law assessment and turnover-based merger thresholds can effectively answer to all of the emerging competition policy challenges in the digital economy.

Article 20 GDPR introduces the new data subject right to data portability. Originally targeted to social network operators, the provision is increasingly relevant also for other data controllers operating in the digital sector. Although aiming at providing a basis for a high level of data protection, encouraging competition among digital service providers and strengthening data subjects’ control over the use of
personal data, the right to data portability is likely to create competition concerns especially in the context of article 102 TFEU which prohibits the abuse of dominance in the European Single Market. Since the balance of bargaining power in the digital marketplace is not always equal between data controllers and individual data subjects, potential abusive and unfair business practices may emerge. Partly for this reason, the right to data portability appears to build an essential link between data protection regulation and competition law assessment in the EU.

The general aim of the thesis is to illustrate and critically assess the increasingly visible role of different EU law regimes in the competitive assessment of the digital markets. The research focus of this study is primarily on the intersection between data protection and competition rules in the European Union. By analysing some of the recent development trends and emerging data protection concerns in EU Member States and in the decisional practice of the European Commission, this thesis seeks to highlight the growing importance of data protection considerations in the competitive assessment of national competition authorities, national courts, the European Commission and the CJEU.

**Nyckelord:**

EU-rätt; dataskyddsreglering; den allmänna dataskyddsförordningen; artikel 20 GDPR; rätt till dataportabilitet; artikel 102 FEUF; konkurrensrätt; missbruk av dominerande marknadsställning; kontroll av företagskoncentrationer.

EU law; GDPR; data protection law; article 20 GDPR; right to data portability; competition law; article 102 TFEU; abuse of dominance; article 102 TEUF; merger control; big data.
# TABLE OF CONTENTS

Abbreviations............................................................................................................................................................................. 1

1 INTRODUCTION........................................................................................................................................................................ 1
1.1 Protecting free competition and personal data in the digital economy ............. 1
1.2 The research questions and methodology................................................................. 3
1.3 Structure.................................................................................................................................................................................... 5
1.4 Notes on terminology............................................................................................................................................................... 5

2 THE REFORM OF EUROPEAN DATA PROTECTION LAW .......... 8
2.1 The history and development of data protection in Europe ......................... 8
2.2 The General Data Protection Regulation (GDPR) ........................................ 10
   2.2.1 Scope of material application ........................................................................... 11
   2.2.2 Anonymization and pseudonymization .......................................................... 14
   2.2.3 Legal justifications for processing of personal data ......................................... 16
       2.2.3.1 Personal data processing based on consent ............................................... 16
       2.2.3.2 Other statutory permissions under article 6 GDPR ................................. 18
2.3 The challenges of Big Data for the European data protection legislation .... 20
   2.3.1 Compliance with the basic data processing principles ...................................... 22
2.4 The intersection between data protection and competition rules in EU law .... 24

3 ASSESSMENT OF MARKET POWER IN THE DATA-DRIVEN ECONOMY .............................................................. 28
3.1 Digital business models: important concepts and functionalities ............... 28
   3.1.1 Examples of multi-sided businesses .................................................................. 28
       3.1.1.1 Social networks .......................................................................................... 29
       3.1.1.2 E-commerce platforms .............................................................................. 30
       3.1.1.3 Search engines .......................................................................................... 31
3.2 Definition of relevant market ............................................................................ 32
   3.2.1 The relevant product market ............................................................................. 33
   3.2.2 The relevant geographic market ......................................................................... 34
   3.2.3 Defining the relevant market for personal data ................................................. 35
3.3 Definition of market power ............................................................................... 36
   3.3.1 Conceptual issues and methods of assessment ................................................. 36
       3.3.1.1 Actual competitors ..................................................................................... 39
       3.3.1.2 Potential competition and barriers of entry ................................................ 41
3.3.2 Personal data as a source of market power .................................................42
3.3.3 The second Facebook/WhatsApp merger procedure [2017] ....................45
3.4 Preliminary conclusions on chapters 2 and 3 .............................................47

4 BIG DATA AND MERGER CONTROL: MARKET DEFINITION, MARKET POWER AND DATA PROTECTION CONSIDERATIONS ...49
4.1 On the nature of data-driven mergers .......................................................... 49
4.2 Decisional practice of the European Commission ....................................... 50
  4.2.1 Google/DoubleClick [2008] .................................................................. 51
  4.2.2 Microsoft/Yahoo Search Business [2010] ............................................. 52
  4.2.3 Microsoft/Skype [2011] ...................................................................... 54
  4.2.5 Facebook/WhatsApp I [2014] ............................................................... 55
  4.2.4 Publicis/Omnicom [2014] .................................................................... 57
  4.2.6 Sanofi/Google [2016] ......................................................................... 57
  4.2.7 Microsoft/LinkedIn [2016] ................................................................. 59
4.3 Emerging data protection and privacy issues in merger control .................. 60

5 THE RIGHT TO DATA PORTABILITY IN THE CONTEXT OF EU COMPETITION LAW ........................................................................63
5.1 The right to data portability under article 20 GDPR ................................... 63
  5.1.1 Scope of application, exercise of the right and rationale ....................... 63
  5.1.2 Exclusion of the right to data portability ............................................. 65
5.2 Abuse of dominance under Article 102 TFEU ........................................... 66
  5.2.1 The concept of abuse of dominance .................................................... 66
  5.2.1 Exclusionary non-pricing abuses under article 102 TFEU ................. 67
    5.2.2.1 Refusal to supply ......................................................................... 69
    5.2.2.2 The essential facilities doctrine in EU law ................................ 70
  5.2.2.3 Data as an essential facility ........................................................... 74
5.3 Applicability of EU competition rules to data portability ......................... 77
  5.3.1 The EC investigations into Google ...................................................... 78
  5.3.2 The Facebook investigation in Germany [2016-2018] ....................... 80
5.4 The concept of fairness in the digital sector ............................................... 82
  5.4.1 The controversial nature of personal data ....................................... 82
  5.4.2 Fairness of personal data processing ................................................. 84
  5.4.3 The requirement of consent and unfair digital trading terms ............ 85

6 CONCLUSIONS ...............................................................................................89
LIST OF REFERENCES ................................................................. 101

Literature .................................................................................. 101
Case law (CJEU) ........................................................................... 125
Case law (General Court) .............................................................. 131
Court proceedings (General Court) ................................................. 133
Opinions of Advocate General ..................................................... 134
Decisions (European Commission, DG Comp) ............................... 134
Decisions of the French Competition Authority .............................. 136
Decisions of the Belgian Competition Authority ......................... 136
Decisions of the Italian Competition Authority ................................ 137
The Federal Court of Justice of Germany ................................. 137
The Federal Constitutional Court of Germany ........................... 137
The District Court of Berlin ......................................................... 137
The Supreme Court of the United States .................................... 137
Dictionaries .............................................................................. 137
Primary Legislation .................................................................... 137
Secondary legislation .................................................................. 138
Press Releases ........................................................................... 139
Other Official Sources ................................................................. 140
Speeches ................................................................................... 144
Newspapers / News websites ....................................................... 145
Web material ............................................................................. 145
Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGCM</td>
<td>Autorità Garante della Concorrenza e del Mercato (Italian Competition Authority)</td>
</tr>
<tr>
<td>B2B</td>
<td>Business-to-business</td>
</tr>
<tr>
<td>B2C</td>
<td>Business-to-consumers</td>
</tr>
<tr>
<td>BDSG</td>
<td>Bundesdatenschutzgesetz (The Federal Data Protection Act of Germany)</td>
</tr>
<tr>
<td>BGH</td>
<td>Bundesgerichtshof (The Federal Court of Justice of Germany)</td>
</tr>
<tr>
<td>BVerfG</td>
<td>Bundesverfassungsgericht (The Federal Constitutional Court of Germany)</td>
</tr>
<tr>
<td>C2C</td>
<td>Consumer-to-consumer</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>DG Comp</td>
<td>Directorate-General for Competition (EC)</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPD</td>
<td>The Data Protection Directive 95/46/EC</td>
</tr>
<tr>
<td>DSM</td>
<td>Digital Single Market</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECFR</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EUMR</td>
<td>European Union Merger Regulation</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission / Federal Trade Commissioner</td>
</tr>
<tr>
<td>GDPR</td>
<td>The General Data Protection Regulation (EU) 2016/679</td>
</tr>
<tr>
<td>GWB</td>
<td>Gesetz gegen Wettbewerbsbeschränkungen (German Act against Restraints of Competition)</td>
</tr>
<tr>
<td>IoT</td>
<td>The Internet of Things</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium-sized Enterprises</td>
</tr>
<tr>
<td>SSNIP</td>
<td>Small but Significant Non-transitory Increase in Price</td>
</tr>
<tr>
<td>TEU</td>
<td>The Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>The Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>VZBV</td>
<td>Verbraucherzentrale Bundesverband (The Federation of German Consumer Organisations)</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Protecting free competition and personal data in the digital economy

Digitalization is changing traditional market conditions and this rapid technological development is likely to affect both economic operators, and consumers as individuals. Internet of Things devices and new digital business models are gaining ground and reforming our understanding of markets for products and services. Networked technologies such as smart products and efficiency applications often communicate with each other via the Internet. As a result, this frequent interaction creates a network of data collection and usage activities. In the digital environment where companies increasingly seek to benefit from personal data in their business practices, it is necessary to consider the different dimensions of the personal information acquired, processed and monetized in competitive markets. Being at the heart of digital goods and services, data are likely to have an impact on international trade and play a key role in the modern economy.

In the European Data Economy where a multitude of different market players operate, many of the digital products and services offered online are seemingly free of charge. However, the personal data of individual consumers is often considered a counter-performance for the products and services provided by companies. The extensive economic exploitation of data processing activities by companies especially in the digital context clearly indicates that personal data are a valuable asset worth investing in. Thus, the concepts of revenue and currency are developing and new data-related business models emerge. In addition to the economic dimensions of personal data, it is important to recognize that the concept also has a more dignified dimension as a fundamental right protected by the EU data protection rules and the Charter of Fundamental Rights of the European Union. The relevance of this aspect is growing in the digital economy and is also likely to require increasing interaction between different EU law regimes.

1 In this thesis, the terms data subject, consumer, individual and user are all used synonymously within the meaning of article 4 GDPR.
2 In the European Union, the digitalization process is related to the concept of the Digital Single Market. This policy introduced by the European Commission originally in 2015 aims at maximising the positive impacts of digitalization on individuals and European business activities in the European Single Market (see DSM Strategy 2017 review, p. 4 and Themelis 2013, p. 2-4). For an analysis of the impact of the DSM Strategy on audio-visual industry, see Tobias 2016 and on antitrust issues Batchelor 2015.
3 For example, Costa-Cabral and Lynskey argue that in addition to business and property related aspects personal data also has a dignitary dimension (see art. 8 ECHR, right to data protection). This fundamental right is partly protected through data protection legislation (Costa-Cabral 2017, p. 12).
4 In accordance with the reform of EU Data Protection legislation, the EC introduced the concept of the European Data Economy in its Communication "Building a European Data Economy (10.1.2017). The concept refers to the measurement of the impacts of the data markets on the economy as a whole (p. 2).
5 For example, Malgieri 2017, p. 1-2.
7 Graef 2016A, p. 129-130. According to Graef, the fact that firms have started to offer consumers possibilities to partly replace the monetary payment for a product or service by giving their permission to personal data collection seems to illustrate the emergence of a new kind of currency.
8 See for example Savin 2017, p. 266-268 and Rees 2013.
Although traditional customer data have long been essential for private business purposes, the large quantities of data sets created in the digital economy cannot usually be managed or analyzed with traditional methods. In order to draw value from this untouched information (so-called raw data), new innovative techniques need to be applied. As the frontiers of innovation and science are expanding, it seems to be important to consider the economic and consumer-related risks that the commercial use of data is likely to pose. The current challenges surrounding personal data and data processing issues are closely related to the key concepts of big data and the Internet of Things (IoT).

Partly against the above-mentioned background, it is natural that the data protection legislation of the European Union is going through a reform. Consequently, European data protection standards are becoming increasingly high. As the product of a legislative process lasting more than four years, the new General Data Protection Regulation 2016/679 of the EU (GDPR) which comes into force in May 2018 will have a global impact on the use, collection and sharing of personal information. It also sets great emphasis on privacy and security and institutes rules applicable in all Member States of the EU by significantly deepening and broadening the range of obligations that actors, especially the data controllers must comply with. Although a result of an EU harmonization procedure, the territorial scope (art. 3(1) GDPR) of the new legal instrument is not only limited to EU boundaries. With its transnational application, also the effective and fair competition shall be ensured in the EU internal market.

The fast progress of information technology is likely to facilitate the exchange and processing of personal data. However, the characteristics of digital markets often differ from the traditional offline business environment and business practices. Digital business models are closely linked to the notion of digital platform. For example, an important characteristic of this concept is the interaction between two user groups (e.g., users and advertisers or buyers and sellers). As data volumes in these economic sectors are increasing, the need for access and analysis of user data is becoming a prominent part of firms’ business strategies. The level of concentration is high in many digital

---

9 The concept of digital economy can be understood referring to markets that focus on digital technologies, such as communication, IT and data processing. These activities often involve trading of information goods or services through electronic commerce (Capobianco 2017, p. 2 and OECD 2012).
11 Voigt 2017, p. 1. Europe is traditionally seen to have a strong rather than a detailed regulatory regime for data protection and privacy issues (Jørgensen 2017, p. 108).
12 The European Commission originally proposed the legislative package in 2012 (Díaz Díaz 2016, p. 209).
13 The new GDPR replaces the previous data protection legislation (Data protection Directive 95/46/EC).
14 Ustaran 2016, p. 3-5.
15 Bräutigam 2012, p. 435. The article 20 GDPR introduces a new data subject right, the right to data portability. The GDPR addresses this issue not only from the perspective of individual users, as it is important for all stakeholders, such as businesses. However, Vanberg argues that art. 20 GDPR cannot sufficiently ensure data portability and has to be supplemented by existing EU competition law provisions, especially article 102 TFEU (Vanberg 2017, p. 2 and 7).
16 Voigt 2017, p. 22. See also recital 9 GDPR. The previous fragmentation of the European data protection legislation and legal uncertainty in EU Member States were considered an obstacle to economic activities and to lead to distortion of competition.
18 For an overview of competition in the digital economy, see the website of the German Fedderal Cartel Office (Bundeskartellamt), section Economic sectors – Digital Economy (visited 21.1.2018).
markets, such as the market for search engines. Although the EU data protection legislation and policy aims at ensuring the free flow of personal data, critics argue that this framework cannot effectively tackle the challenges of current data protection practices. It can also be argued whether the massive data collection by many IoT devices is likely to present an unrealistic and unfair entry barrier for smaller firms, effectively enforcing the oligopoly amongst the more dominant digital service providers.

Corporate and commercial rivalry in the European Single Market is subject to the application of EU Competition Law. Competition regulation and enforcement in Europe aims at ensuring the fair competition, economic efficiency and the elimination of obstacles concerning the four freedoms of the European Single Market. Traditionally, the use of personal data has not been seen as an essential part of competition law assessment. In many cases, competition law and data protection legislation have been considered to pursue different goals. In addition, data protection rules have not been understood falling within the scope of competition law enforcement. However, one of the main arguments of this thesis is that EU competition law should not be assessed completely in isolation from other regimes of EU law. The recent practice of the European Commission (DG Comp) in the field of merger control, academic research and political discussion as well as the potential for CJEU case-law clarifying the privacy concerns of anti-competitive practices in the digital economy indicate the need for further assessment of these aspects.

### 1.2 The research questions and methodology

The main objective of this thesis is to assess and analyze the reform of the EU data protection legislation and its impact on the regulation and enforcement of competitive markets. The scope of legal assessment is mainly limited to the European context. However, as digital markets are increasingly global, many of the concepts and cases discussed also have a broader dimension exceeding the external borders of the EU. In the digital economy, the emergence of new business models is often closely related to the commercial use of personal data. In order to be able to assess the risks of breaches of EU competition law in the data-driven economy, it is important to understand the different dimensions of personal data and the more generally the value of data as a business asset for companies operating in the European Single Market.

---

20 Koops 2014. Ezrachi and Stucke argue that there is a growing mistrust of the big data and big analytics, especially concerning the methods used by companies. In order to be beneficial for consumers, online markets and related firms must be trusted by individuals (Ezrachi 2016B, p. 243).
21 Kulwijk 2016, p. 5.
22 The four freedoms of the EU include the free movement of goods, services, persons and capital (Whish 2015A, p. 52-53 and Raitio 2016, p. 266-267). Competition law is an essential element for the attainment of four freedoms as they only can be attained if firms can freely compete within the EU (Rodger 2008, p. 101). See also Wise 2007.
23 For the normative foundations of competition law, see Maier-Rigaud 2012. According to Whish, it is necessary to read the EU competition rules in the context of the objectives and principles of the TFEU and TEU (Whish 2015A, p. 53).
24 See for example Kemp 2014, p 488 and Vezzoso 2012.
As the provisions of the GDPR seek to enforce privacy and personal data protection, a reasonable balance between both data protection and competition law aspects is maintained when discussing these issues. By using some of the relevant legal concepts and tools of competition law as well as with the help of the existing data protection legislation, the aim of this thesis is to answer, at least, the following research questions:

1. **What is the current state of data protection legislation in the European Union and what are its main challenges in relation to competition in the data-driven markets?**

2. **What is the competitive significance of big data for digital businesses and how can the use of personal data reflect the business practices of a company?**

3. **What are the characteristics of the most relevant digital business models and their primary risks associated with data protection and competition law enforcement?**

4. **Can personal data have an impact on an undertakings market power? What are the primary anti-competitive concerns associated with the right to data portability introduced by article 20 GDPR?**

5. **Is there an essential link between EU data protection law and competition law? How and to what extent should the data protection and privacy considerations be included in the competition law assessment?**

The nature of this thesis is both practical and theoretical. Although recent case law is used to analyze and illustrate the recent trends in the decisional practice of the European Commission and the CJEU, especially the competition concerns require a theoretical approach, to some extent. In addition to case study, recent academic literature, legal commentaries and official documents are used in the assessment of the research questions.

To support the theoretical analysis of the thesis, some of the central notions and concepts of law, economics and technology are clarified. An essential aim of this study is to examine, evaluate and, to some extent, even predict the challenges that data protection law, competition law regulation and enforcement authorities will face in the upcoming years. In this respect, the approach adopted in the thesis is largely misuse-oriented and therefore some of the current de lege ferenda debates in the EU are also reflected. With a normative approach to some of the central provisions and principles of the GDPR, the first part of the thesis seeks to build a basis for the assessment of relevant personal data related competition concerns in chapters 4 and 5. Therefore, the methodological aim of this thesis is partly to systematize and interpret the existing legal norms and other sources of law.

The amount of case law concerning the data protection concerns related to competition law regime is somewhat limited since traditionally the data protection and privacy issues have been considered separate from competition law assessment. For this reason, the nature of this thesis is also relatively forward-looking. However, the
decisional practice of national competition and consumer authorities in the EU Member States is also presented as it can potentially provide relevant indications of the future developments at the EU level.

1.3 Structure

As collection, processing and commercial exploitation of personal data are central features of modern digital business practices, it is necessary to discuss some of the data-related theoretical and conceptual aspects before moving towards a more practical analysis. Therefore, chapter 2 discusses the current reform of EU data protection legislation. In order to give the reader a general view of the GDPR, some of the key provisions and structural features of the regulation are clarified.

In chapter 3, some of the general concepts and principles of EU competition law and policy are presented in the light of relevant CJEU case law and the decisional practice of the European Commission. After the introductory part, the chapter discusses some of the relevant concepts related to article 102 TFEU. Important notions, such as relevant market, market power and potential competition, are clarified and further discussed in the context of digital and data-driven markets. The preventive and forward-looking nature of the EC merger control procedure requires somewhat theoretical approach to these concepts. As the market concentration in many digital sectors is relatively high, the chapter 4 focuses on EU merger control and related data protection and privacy concerns. Many of the recent data protection issues concern online platforms. For this reason, the market definition of online platforms is discussed and the latest case law and decisional practice of the European Commission (DG Comp) and the CJEU are analysed.

The chapter 5 focuses on the right to data portability introduced by article 20 GDPR. This new data subject right is closely linked to the potential risks concerning the abuse of dominance and this provision also builds an important link between data protection and competition law in this section of the thesis. The chapter 6 summarizes the material assessment of the study and returns to the research questions presented in the introductory chapter 1.

1.4 Notes on terminology

In the European Union, the interaction between common European law and the official languages of the EU Member States may create challenges for the cooperation between different stakeholders. For this reason, the harmonization of legal terms within the EU has been one of the means to facilitate this interaction.25 In addition to the general terminology of EU law, several more technical and non-legal concepts are used in the thesis requiring further clarification. Many of the terms used in this thesis are international and as the English language can be considered, despite the prospective

---

withdrawal of the United Kingdom from the EU, the modern *lingua franca*\(^{26}\) of the European community, they might not even have national equivalents.

*Data protection* refers to protection activities of data from destruction, corruption or misuse. In legal context, it is used to denote especially the regulation of use of and access to *personal data*.\(^{27}\) The concept of data protection can also been seen as part of the *right to privacy*, which in turn refers to a state of limited accessibility.\(^{28}\) According to article 4(1) GDPR, ‘personal data’ can be understood encompassing any information relating to an identified or identifiable natural person (*data subject*).\(^{29}\) Therefore, data are considered personal if the identification (e.g. detection directly or indirectly) of a person is possible with the data available.\(^{30}\)

According to the article 4(1) No. 7 of the GDPR, a *controller* (or *data controller*) is ‘a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data’. This notion is identical with the definition of the Data Protection Directive. The legal form of the controller is not decisive when defining the legal obligations under the GDPR. As the GDPR does not provide for an *intra-group exemption*, each entity is considered a controller and consequently each company is only responsible for the data processing that takes place under its controllership.\(^{31}\) A *processor* (or *data processor*) is ‘a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller’ (article 4(1) No. 8 GDPR). As in the case of controllers, the legal form is not decisive. The activities and existence of a processor depend on the decisions of the controller. Thus the data processing can take place within the controller organization or it can be delegated to an external entity also regarded as a ‘processor’.\(^{32}\) However, if the processor exceeds his mission and acquires a relevant role in the determination of data processing activities, he will be considered a *joint controller*.\(^{33}\)

*Big Data* (or *big data*) denotes data of a very large size. Typically the management and manipulation of these large data sets is logistically challenging. In technology, the term can also be used to describe the branch of computing that involves such data.\(^{34}\) The use of different innovative techniques enables the commercialization of *raw data* (or *primary data*), which refers to the unprocessed form of big data collected from the source.\(^{35}\) It should be noted that the concept of *big data* includes all kinds of

---

\(^{26}\) Ristikivi 2005, p. 199-200. The writer argues that while English is widely used by lawyers from different Member States, it lacks the essential characteristics of a *legal lingua franca* of the EU, as it is the language of *common law system*.

\(^{27}\) Oxford English Dictionary, online version (Oxford University Press). The article 8 of the Charter of Fundamental Rights of the European Union (ECFR) can be seen as the cornerstone of this right. For the concepts of personal data and sensitive personal data, see also De Hert 2016, p. 183-184.

\(^{28}\) Bygrave 2003, p. 420.

\(^{29}\) OECD Digital Economy Paper 2013, p. 7. See also Stucke 2016, p. 15. For the notion of data subject, see for example Blume 2015.

\(^{30}\) Voigt 2017, p. 11.

\(^{31}\) Ibid., p. 17-18.

\(^{32}\) For example, processors could be computing centres or cloud computing suppliers. For data protection challenges for cloud computing, see Vidovic 2016.

\(^{33}\) Ibid., p. 20.

\(^{34}\) Oxford English Dictionary, online version (Oxford University Press). See also Wang 2017, p. 601-602.

unprocessed information and it is not limited to the different types of personal data. The value from big data is acquired through the methods of big analytics. As a branch of data analytics it can be defined as technical means to extract valuable information from data and to provide tools to influence, understand and control the data objects.36

The Internet of Things (IoT) is a frequently used term describing all the devices communicating with each other and with individuals and companies via the Internet. In the modern digital context, the notion of the IoT can be understood encompassing basically all products and services such as smart devices, banking services and medical technology.37 A common feature of the various definitions of the IoT is that processing of personal data is considered an essential part of this term.38

In the context of computing and mathematics, an algorithm can be understood as a set of rules or procedure used especially in problem solving and calculation. Alternatively, it can also refer to a precisely defined set of logical or mathematical operations used to perform a particular task.39 Machine learning refers to the capacity of a computer to learn from experience. In the context of computing, this may refer to activities in which the computer is able to modify its processing on the basis of newly acquired information.40 According to Intel, it could be described as the set of tools and techniques allowing computers to think by creating mathematical algorithms from the basis of accumulated data.41

A platform refers to standard system architecture in computing. It also refers to a certain type of machine or operating system considered to be the base on which different software applications are run.42 The notion covers a variety of different online activities such as online advertising platforms, search engines, social media as well as communications services. According to the European Commission, the key characteristics of online platforms include the ability to shape and create new markets, their benefits from network effects43, operation in multisided markets44, importance in digital value creation and the reliance on information and communications technologies.45 Hence, online platforms act as intermediaries between customer groups constructing an essential part of the network economy.46

---

36 OECD Data-Driven Innovation Report 2014, p. 4. Also Stucke 2016, p. 16. According to Stucke and Grunes, the essential features, so-called four V’s of Big Data are volume, velocity, variety and value (sometimes veracity).
37 Treacy 2013, p. 11. A British technology pioneer Kevin Ashton first introduced this relatively trendy term during his presentation in 1998 (see Santucci 2009, p.2).
38 Stucke 2016, p. 15-16. See also Corbet 2015.
39 Oxford English Dictionary, online version (Oxford University Press).
40 Ibid.
42 Oxford English Dictionary, online version (Oxford University Press).
43 The notion of a network effect (alternatively network externality) refers to the increase in the value of a product or service when the number of other users consuming this product increases (Whish 2015, p. 11). They are possibly the most common source of market power in high-tech industries. For an overview of the topic, see for example Lemley 1998.
44 A multi-sided (or two-sided) market can be defined as a business environment in which there are two or more user groups providing each other with network benefits. Typically a network effect rises as more consumers join some side of the platform (Whish 2015, p. 12). See also Graef 2016A, p. 39-35.
2 THE REFORM OF EUROPEAN DATA PROTECTION LAW

2.1 The history and development of data protection in Europe

Although the relative novelty of data protection at EU level and the close relation to technological development, the origins of data protection legislation in Europe can be traced back to the period after the World War II and the reforming of the new German constitution.\(^{47}\) In order to prevent power shifts between various government branches, the first data protection laws, such as the 1970 Hessian Privacy Protection Act, emerged in the Western Europe.\(^{48}\) The constitutional development in West Germany reflected the acknowledgement of information as the basis for almost all public and private activities. In West Germany, the growing concern of the possible dissemination and manipulation of personal information by the government or private economic operators without the knowledge of the data subject resulted in the first federal data protection act in 1977, Bundesdatenschutzgesetz (BDSG).\(^{49}\)

The first generation of data protection laws in the 1970s was enacted in a world where automated data processing technology was not yet widely used.\(^{50}\) Only certain government bodies and some of the major companies had the opportunity to act as data controllers. The general purpose of these early data protection rules was mainly to limit the state's power and ensure the transparency of public databases. However, the rapid development of information technology in the 1980s and 1990s challenged the existing national legal frameworks. The spread of IT devices such as personal computers and later internet connectivity as well as the emergence of new online business models and techniques made the private demand for personal data usage at least equal to the public use.\(^{51}\)

Since 1995, the processing of personal data has been subject to the obligations under the general EU Data Protection Directive 95/46/EC (DPD). It was the first legislative instrument harmonizing national data protection laws within the EU.\(^{52}\) At this time, different national levels of data protection could not provide legal certainty for data processors, controllers or individual data subjects.\(^{53}\) Even so, the first efforts to create a common European data protection directive had taken place already in 1976.\(^{54}\) This slow process may have reflected the challenges that the growing European Community

\(^{47}\) The first legal provisions protecting privacy in Germany were included in the articles 1 and 2 of the German Constitution of 1949 (Grundgesetz). These rules protected the ‘dignity of individual’ and the ‘right to the free development of one’s personality’. In data protection context, see Case C-377/98 Netherlands v Parliament and Council [2001] ECR I-7079, para. 70. Human dignity as a general principle in EU law was confirmed in Case C-36/02 Omega Spielhallen [2004], ECR I-9609, paragraphs 32 and 34 and more recently in Case C-34/10 Brüstle [2011] ECR I-09821, paragraphs 30, 34 and 35.

\(^{48}\) Bennett 1992, p. 75. See also Kiss 2015, p. 313-314. The Hessian Data Protection Act served as an example for the legislative development also in other European countries, such as Sweden (1973) as well as Denmark, Norway and France (1978).

\(^{49}\) See Riccardi 1983, p. 244-245.

\(^{50}\) Rugard 2012, p. 6.

\(^{51}\) Kiss 2015, p. 313-314.

\(^{52}\) Wong 2012, p. 229-230.

\(^{53}\) Voigt 2017, p 1-2.

\(^{54}\) EC Communication on protection of personal data 13.9.1990, p. 3.
was facing in the years when national data protection frameworks were still in the early development stages. Originally modelled on the Council of Europe Convention on data protection, the directive contained several provisions new to many national data protection regimes and aimed at harmonizing the relatively fragmented European legislation. Striving to achieve a balance between individuals and personal data users, it increased the regulation of the rights and obligations of both data subjects and data processors.

Although the EU Member States were mostly able to implement the DPD by either amending existing national legislation or introducing new laws, the difficulties in the application of the directive and some of its unclear concepts resulted in national court proceedings. In the CJEU judgement C-101/01 Lindqvist [2003], the scope, meaning, application and definition of the DPD were challenged for the first time. In its decision, the Court assessed the alleged violation of the Swedish personal data protection law by a church employee (catechist). One of the main questions concerned the applicability of the Data Protection Directive online. The CJEU concluded that the act of referring online (on an Internet page) to identified persons or their activities, constituted the processing of personal data within the meaning of the article 3(1) DPD. Several changes were made to the Swedish data protection laws after the judgement and a misuse-oriented national approach was adopted. The Lindqvist case confirmed the understanding that the DPD applied to information concerning individuals and permitted their right of action as well.

When the Data Protection Directive was introduced in 1995, the Internet was still in its infancy. Hence, the need for a provision governing the vast amounts of personal data transferred worldwide was relatively limited. From the middle of the 1990s, the establishment of the information society became an important political goal in the European Union. Building the trust in the field online services, especially in the legal regulation of increasingly globalized personal data processing and privacy became important elements of this rather vaguely defined phenomenon. As the case law of the CJEU concerning the scope, implementation, application and interpretation of the DPD indicates, there were considerable shortcomings in the application and understanding of the Directive on the national level. During the last few years, the European

---

59 Case C-101/01 Lindqvist, ECR 2003 I-12971, para. 27.
60 Wong 2012, p 230.
61 Garcia 2005, p. 1230. The direct applicability of the DPD was assessed in the following CJEU cases: Joined cases C-465/00 and C-138/01 Rundfunk [2003], ECR I-04989, para. 98 and Joined Cases C-468/10 and C-469/10 ASNEF [2011], ECLI:EU:C:2011:777, paragraphs 52-55.
62 According to Lynskey (2015, p. 4), at the time when the DPD was adopted, only 1% of the EU population used the Internet. For a brief history of Internet, see Kagan 2010, p. 274-276.
63 Voigt 2017, p. 170.
64 Kiss 2015, p. 314.
65 In 2001, after the action brought by the European Commission, the CJEU found that the Duchy of Luxembourg had failed to adopt the laws, regulations and administrative provisions in order to comply
discussion has largely focused on the need for clarification and the possible improvements of the data protection framework of the EU. For example, the application of data protection rules on certain more or less opaque business models such as cloud computing and behavioural advertising seemed to need further consideration.\textsuperscript{66}

The significant social, cultural and economic changes in the EU during the last couple of decades culminated in the introduction of the General Data Protection Regulation 2016/679 of the EU (GDPR) in 2016.\textsuperscript{67} Entering into force in May 2018, it is perhaps the most comprehensive and forward looking legislative instrument in the digital era and the guiding tool of the European data protection efforts at least for the next few decades. Of all the challenges it most likely will face, the emergence of big data might be the greatest.\textsuperscript{68} Big data analysis is becoming mainstream\textsuperscript{69} and many of the data-driven business models, often involving multi-sided platforms, are used to create a competitive advantage over the rivals.\textsuperscript{70} While striving to maintain a balance between efficient data-based innovation, sufficient personal data protection of individuals and fair competition in a rapidly changing environment, the long-term effects of the GDPR remain still uncertain.

\subsection{The General Data Protection Regulation (GDPR)}

As a directly applicable legal instrument of the EU, the GDPR requires no further implementation measures by EU Member States. The legal framework created by the regulation maintains the basis of the previous DPD and adds certain elements to it.\textsuperscript{71} It aims at clarifying the existing obligations and rights while providing new rules improving enforcement efforts and legal compliance in the EU. It should be noted that when interpreting the provisions of the DPD and the GDPR, the fundamental rights to privacy and data protection of the ECFR (art. 7 and 8) as well as the article 8 EHRC (right to respect for private and family life) shall also be taken into account.\textsuperscript{72}

with the DPD (Case C-450/00 Commission v Luxembourg [2001], ECR I-07069). See also the following cases concerning the failure of a Member State to fulfil the obligations under article 28(1) no. 2 DPD: C-518/07 Commission v Germany [2010], ECR I-01885 and Case C-614/10 Commission v Austria [2012], ECLI:EU:C:2012:691.


\textsuperscript{67} Kiss 2015, p. 315-316. With the adoption of the Treaty of Lisbon in 2009, article 16 TFEU enabled explicit legal grounds to enact data protection legislation.

\textsuperscript{68} Zarsky 2017, p. 996.

\textsuperscript{69} NewVantage Partners LLC, ‘Big Data Executive Survey 2016: An Update on the Adoption of Big Data in the Fortune 1000: Executive Summary’ (2016), p. 2. Only 5,4 % of firms involved in the 2016 survey reported that they did not have any big data related initiatives planned or underway (p. 5).

\textsuperscript{70} Stucke 2016, p. 38.

\textsuperscript{71} For the changes in data subject rights in the GDPR, see Doherty 2017. See also Davies 2016, p. 290-291. Davies (the founder of Privacy International) argues that the new legal framework falls short from its original promise by offering enormous potential but lacking the detailed mechanisms required.

\textsuperscript{72} Costa-Cabral 2017, p. 16. For example, see the following cases: Joined Cases C-293/12 and C-594/12 Digital Rights Ireland [2014], OJ C 175, 10.6.2014, p. 6-7, paragraphs 29, 32, 34-37 (articles 7, 8, 11 ECFR)
Since one of the central aims of the European Union has been to strengthen people's trust in the responsible treatment of personal data\textsuperscript{73}, the new regulation imposes new obligations deepening and broadening the range of obligations that data controllers must comply with.\textsuperscript{74} The most important data protection obligations under the GDPR can be divided into two main categories: organization requirements\textsuperscript{75} and requirements concerning the lawfulness of data processing activities\textsuperscript{76}.

### 2.2.1 Scope of material application

The General Data Protection Regulation is applied to any processing of personal data.\textsuperscript{77} Therefore, any establishment processing or controlling the processing activities related to personal data will be in the scope of application of the GDPR.\textsuperscript{78} Considering the great economic value of data, companies having data as their key asset will be especially affected.\textsuperscript{79} According to the article 2(1) GDPR, the material scope of the regulation covers data processing activities by wholly or partly automated means. The GDPR is also applied to non-automated means forming or intended to form a filing system.

The article 2(2) GDPR contains four exceptions limiting the material scope of application of the regulation. These are the following: security policy, criminal persecution, data processing by a natural person in purely personal or household activities and the data processing by competent authorities in certain criminal law and public safeguard measures. According to Voigt, the exception concerning personal and

---

\textsuperscript{73} For the definition of 'personal data' (art. 2(2) DPD), see the following cases: Case C-615/13 P PAN Europe [2015], ECLI:EU:C:2015:489, para 29; Case C-28/08 Bavarian Lager [2010], ECR I-06055, para. 68; Joined Cases C-141/12 and C-372/12 M [2014], OJ C 315, 15.9.2014, p. 2-3, paragraphs 34, 38-41; Case C-291/12 Schwartz [2013], ECLI:EU:C:2013:670, para. 27; C-342/12 Worten-Equipamentos [2013], ECLI:EU:C:2013:355, para. 19; Case C-473/12 Englebert [2013], OJ C 9, 11.1.2014, para. 26; Case C-212/13 Ryneš OJ C 46, 9.2.2015, p. 6-6, para. 22; Case C-615/13 P ClientEarth [2015], ECLI:EU:C:2015:489, paragraphs 29-33; Case C-201/13 Smaranda Bara [2015], ECLI:EU:C:2015:638, para. 29; Case C-13/16 Rigas satiksme [2017], ECLI:EU:C:2017:336, para. 24; Case T-259/03 Kalliopi Nikolau [2007], II-00009, para. 222; Case T-161/04 Jordana [2011], II-00215, para. 91; Case T-496/13 McCullough [2015], ECLI:EU:T:2015:374, para. 66.

\textsuperscript{74} Voigt 2017, p. 2 and Braütigam 2012, p. 435.

\textsuperscript{75} For the definition of controller, see the following cases: Case C-131/12 Google Spain [2014], OJ C 212, 7.7.2014, p. 4-5, paragraphs 33-41; Case C-212/13 Ryneš OJ C 46, 9.2.2015, p. 6-6, para. 34.

\textsuperscript{76} See section 1.4. For the definition of controller, see the following cases: Case C-191/15 Amazon EU [2016], ECLI:EU:C:2016:612. In its judgement, the CJEU held that "any real and effective activity, even a minimal one, exercised through stable arrangements" falls within the scope of the concept of 'activities of an establishment' under art. 4(1) a DPD (para. 75).

\textsuperscript{77} Voigt 2017, p. 9 and 17. See also EC Opinion on personal data 2007, p. 3.
household activities is economically the most significant. Including for example leisure activities and the use of a social network for private purposes, it can be justified by the general social opinion. However, if data processing involves both private and business information, the GDPR will be applied. In the context of data protection, the notion of business activity does not require that the activity in question be remunerated. The decisive characteristics of a business activity are the preparatory measures taken, such as personal data trading for other services or marketing measures. This in turn seems to indicate that it is difficult to justify the exemptions by economic interests.

As personal data processing is a key element when applying the GDPR, the question concerning identifiability of a data subject is of great importance. By combining different pre-collected information from the raw data, the identification of individuals is made possible. However, the wording of the GDPR does not provide further information on the question concerning the actual identifying person of the data subject. This might suggest that the required additional identifying information need not to be in possession of the controller or processor of personal data.

Under the previous data protection framework, all measures that were 'likely reasonably' used for acquisition of additional information from whatever source were considered in the assessment of the potential identifiability. In its judgement C-582/14 Breyer [2016], the CJEU assessed a case where a German politician had accessed several websites operated by public institutions. For security reasons, these websites collected access information, among other things the IP addresses of computers. An action was brought before the national court in order to prevent the Federal Republic of Germany from data processing activities related to the IP addresses of visitors. In its assessment, the Court confirmed the opinion of the Advocate General Campos Sánchez-Bordona stating that the risk concerning the possible identification seemed insignificant, if it required disproportionate effort in terms of cost, manpower and time used (so-called relative criteria).

Although the Breyer judgement concerned the application of the DPD, the GDPR includes indications referring to the continued application of these relative criteria.

---

80 For the notion of ‘data processing for purely personal or household activity’, see the following cases: Case C-101/01 Lindqvist, ECR 2003 I-12971, paragraphs 45-47 and Case C-212/13 Ryneš OJ C 46, 9.2.2015, p. 6-6, paragraphs 28-35.

81 Voigt 2017, p. 16-17.

82 For the definition of processing of personal data, see the following cases: Case C-73/16 Peter Puškár [2017], para. 103; Case C-362/14 Schrems [2015], ECLI:EU:C:2015:650, para. 45; Case C-461/10 Bonnier [2012], ECLI:EU:C:2012:219, para. 52; Case C-131/12 Google Spain [2014], OJ C 212, 7.7.2014, p. 4-5, paragraphs 26-31; Case C-230/14 Weltimmo [2015], ECLI:EU:C:2015:639, para. 37; Case T-320/02 Esch-Leonhardt [2004], ECR I-A-00019; II-00079.

83 Voigt 2017, p. 12. The writers refer to a certain type of information that by itself does not enable the identification of a person but does so in combination.

84 Recital 26 of DPD. See also case C-70/10 SABAM [2011], ECLI:EU:C:2011:771.

85 Case C-582/14 Breyer [2016], ECLI:EU:C:2016:779, paragraphs 13-17.

86 Ibid., para. 46. See also Opinion of Advocate General, 12.5.2016, para. 68. Voigt (2017, p. 13 and recital 26 GDPR) also names technological developments as circumstances taken into account when affirming identifiability of an individual case.

87 Voigt 2017, p. 12. According to Voigt and Van dem Busche, for an example of these indications, the recital 26 GDPR uses terms such as ‘all the means reasonably like to be used’.
According to Borjesius, had the GDPR been applied in the case, it would most likely have reached a similar conclusion. The definition of personal data in GDPR adds certain new examples of identifiers to the one in DPD, such as ‘online identifier’. As IP addresses are online identifiers, it could be rightly argued that IP addresses should be regarded as personal data.\textsuperscript{88} Thus, there was no reason to allow Member States to go outside the scope of the DPD when appealing to fundamental rights.\textsuperscript{89}

In the judgement C-434/16 Peter Nowak [2017], the CJEU assessed the scope of the data subject’s rights to access and rectification as well as the defining features of personal data. The claimant had submitted a data access request after having failed an open book accountancy examination four times and having initially challenged the results. The institute responsible for these examinations denied the request.\textsuperscript{90} Referring to article 2(a) DPD, the CJEU held that the written answers of the candidate at a professional examination, including the comments made by an examiner, constituted personal data.\textsuperscript{91} In contrast, the rights of access and rectification did not extend to the examination questions, which did not as such constitute personal data of the candidate. Member States were allowed to adopt measures restricting these rights, when the restrictions were necessary to safeguard the freedoms and rights of others. Interestingly, the CJEU also interpreted articles 15(4) and 23(1)(e) of the new GDPR stating that the objectives of general public interest of the EU and of a Member State as well as the rights and freedoms of others could not be adversely affected by the data subject’s right to access.\textsuperscript{92} Hence, the CJEU expanded the scope of the notion ‘personal data’ when it found that the expression ‘any information relating to an identified or identifiable person’ of article 2(a) DPD reflected the wide interpretation of this concept.\textsuperscript{93}

In addition to interests of individual data subjects, data protection concerns may rise in cases where data is identifiably related to a group of individuals and group privacy is therefore an increasingly central concept. Recent big data trends also highlight the emerging phenomenon of collective interest as in many cases the data subject affected is a group instead of an individual person.\textsuperscript{94} These groups are often created artificially by analytics.\textsuperscript{95} In the age of big data, data analytics is used to individualize data sets collected by new technologies for business purposes. Even though not all of these data qualify for the purposes of data protection legislation, the potential for random findings has become significant as the processed big data volumes are expanding.\textsuperscript{96}

\textsuperscript{88} Borjesius 2017, p. 136-137. See also EC Opinion on behavioural advertising 2011. Despite the fact that no names can be tied to data, if a company processes personal data in order to single out persons, this can be considered identifying individuals (p. 8).
\textsuperscript{89} De Hert 2017B, p. 28. The ruling in Breyer case was in line with the previous ASNEF judgement (Joined Cases C-468/10 and C-469/10 ASNEF [2011], ECLI:EU:C:2011:777).
\textsuperscript{90} Case C-434/16 Peter Nowak [2017], ECLI:EU:C:2017:994, paragraphs 18-25.
\textsuperscript{91} Case C-434/16 Peter Nowak [2017], ECLI:EU:C:2017:994, para. 62.
\textsuperscript{92} Ibid., paragraphs 58-61.
\textsuperscript{93} Ibid., para. 34.
\textsuperscript{94} Pagallo 2017, p. 44.
\textsuperscript{95} With analytics, Urgessa (2016, p. 526) refers to different information technology related methods. These data processing techniques include for example algorithms, statistics and different mathematical tools used in the collection and identification of data sets. However, genetic data (art. 4(1) No. 13 GDPR) is an example of personal data identifiably related to a group without the contribution of analytics.
\textsuperscript{96} Zwitter 2014, p. 4.
In contrast to traditional profiling and categorization methods using only a few standard variables, data groups set by big data analytics may produce significantly greater predictive capacity because they often utilize hundreds of different variables.\textsuperscript{97} As the members of these groups created by analytics are not usually aware of these activities or their consequences, privacy issues in the big data context can significantly differ from the individual or traditional group privacy issues.\textsuperscript{98} Hence, the examination of collective interest of persons involved in a group may be required in cases where individual identifiability is no longer the defining element for the application of data protection legislation. Collective privacy and data protection as well as the acknowledgement of the emerging group identity concerns could therefore, with good reason, be regarded as the new layer of data protection.\textsuperscript{99}

2.2.2 Anonymization and pseudonymization

The reuse of personal data is an important question and may raise data protection concerns when the purpose of reuse activities differs from the justification of the original collection. When discussing large data sets in the age of big data, balancing the rights and interests of individuals and data processing companies becomes a key issue.\textsuperscript{100} Anonymized data refers to information that cannot be linked to identified or identifiable individuals. Consequently, anonymization\textsuperscript{101} can be understood as modification of personal data in order to remove its connection to an individual. It is often used in statistical or research purposes. Performed effectively, anonymized data does not fall within the scope of the GDPR. However, in many cases the data processor or controller has the possibility to restore this information. If the likelihood of restoration is high enough, the GDPR will be applied.\textsuperscript{102}

Anonymization can be highly beneficial for data controlling and processing entities. Although the total amounts of collected and stored amount of data can be very large, data processing can ultimately focus only on a small part of these datasets. By applying data anonymization measures to the excess data in accordance with the principle of data minimization\textsuperscript{103}, these entities may not meet the numerous compliance and applicability requirements of the GDPR. Thus, data anonymization could also be considered a safeguard tool of privacy.\textsuperscript{104} Nevertheless, the possible risk factors should always be considered in the anonymization processes. The likelihood and severity related to the used techniques and the optimal compliance solution usually require a case-by-case decision. After implementing the optimal anonymization techniques, the

\textsuperscript{97} Typical variables of personal data analytics include age, sex, marital status and place of residence.
\textsuperscript{98} Urgessa 2016, p. 526.
\textsuperscript{99} Mantelero 2016, p. 2.
\textsuperscript{100} Stalla-Bourdillon 2016, p. 285.
\textsuperscript{101} Recital 26 GDPR.
\textsuperscript{102} Voigt 2017, p. 13. Anonymization activities can be divided into two categories: randomization and generalization. The former refers to the modification of data by altering the accuracy and removing the identifiability element from the data. When this randomized information is considered sufficiently uncertain, it is no longer possible to build a connection to an individual. Generalization can be defined as means to dilute or generalize the features of data by modifying the order or scale of data.
\textsuperscript{103} Article 5(1) c GDPR.
\textsuperscript{104} Voigt 2017, p. 14.
controlling entity needs to constantly monitor the situation in order to detect and control the inherent risks, especially the identification potential of the non-anonymized parts of its database.\textsuperscript{105}

The solution concerning anonymous data adapted in the GDPR is still relatively controversial. The potential value of analysed big data sets is gained through the methods of pattern-finding between different data points, whereas the purpose of anonymization is opposite: to dilute and delink the possible relationships between data points in order to make \textit{informational knowledge} non-identifiable. Thus, the key concern seems to be how or to what extent the data processing entities should ensure the balance between effective data anonymization and the high utility of data for possible future disclosure.\textsuperscript{106}

The second method used when personal data are modified to a non-identifiable form is also named in the new GDPR. \textit{Pseudonymization} (art. 4(1) No. 5 GDPR) can be defined as a method of personal data processing in which the data is transformed into a form where \textit{it cannot be attributed to a specific data subject without additional information}. It constitutes one potential measure for data controllers and processors to fulfil the compliance requirements set forth in the GDPR.\textsuperscript{107} It can also be regarded as a response to recent technological advances in the digital economy, offering a “middle ground” solution between fully identifiable personal data in the scope of the GDPR and fully anonymous data.\textsuperscript{108} The definition of pseudonymization is both narrow and broad. For example, certain data processing activities that cannot ensure the non-identifiability of natural persons are left out. For this reason, it seems unlikely that \textit{targeted online advertising} methods will continue to be outside the definition of personal data.\textsuperscript{109} Pseudonymization can be achieved for example by \textit{replacing certain characteristics with other data indicators}. The regulation also requires that the additional information used in the identification is \textit{kept separately} and the pseudonymization process is ensured by additional organizational and technical means. The scope of the GDPR covers pseudonymized data because the re-identification risk is relatively higher than in the case of anonymized data. If used successfully, pseudonymization is an effective way to ensure data privacy.\textsuperscript{110}

\begin{flushleft}
\footnotesize\textsuperscript{105} Voigt 2017, p. 15. \\
\footnotesize\textsuperscript{106} Stalla-Bourdillon 2016, p. 285. \\
\footnotesize\textsuperscript{107} Voigt 2017, p. 15. \\
\footnotesize\textsuperscript{108} Mayer-Schönberg 2016, p 328-329. The \textit{balancing test} in the article 6(4) e GDPR is a concrete example of how pseudonymization can be taken in the account when determining whether and under what conditions it is possible to reuse personal data for new purposes without the usual consent required. \\
\footnotesize\textsuperscript{109} Stalla-Bourdillon 2016, p. 300-301. Given the variety of the information collected by online advertising businesses and the purpose of data processing (analysis of user behaviour), data collected by targeted online advertising should be considered identifiable personal information. \\
\footnotesize\textsuperscript{110} Voigt 2017, p. 15. The writer mentions \textit{encoding} as a possible method of pseudonymization, where the key to the encoded data would be shared only with a limited group of people. 
\end{flushleft}
2.2.3 Legal justifications for processing of personal data

In order to be lawful, the data processing activities of an entity must be legally justified and lawful (art. 6 GDPR).\textsuperscript{111} Compared to the DPD, the GDPR has, in many ways, stricter requirements for the lawfulness of these activities.\textsuperscript{112} By nature, personal data are closely related to individual freedoms and fundamental rights. For this reason, the GDPR also includes certain special personal data categories that are, due to their sensitive nature, subject to stronger protective restrictions (art. 9(1) GDPR).\textsuperscript{113} Many users of digital products such as IoT devices might not be aware of the extent to which data processing is carried out and through which objects these operations are executed. Lack of information and consent can create a barrier for the entities when trying to demonstrate the data subject’s valid consent to processing activities.\textsuperscript{114} The application of the regulation is not dependent on the geographical location of the data processing activities and consequently they need not to take place within the EU.\textsuperscript{115} This may reflect the overall aim of giving the individuals control over their personal data.\textsuperscript{116}

2.2.3.1 Personal data processing based on consent

The basic form of legal justification for the personal data processing is the consent of the data subject (art. 6(1)(a) GDPR).\textsuperscript{117} However, in practice these activities are often based on several legal bases.\textsuperscript{118} As the commercial exploitation of data is increasing and many of the digital products and services are often free to consumers, user consent could also be considered the primary payment mechanism of the companies.\textsuperscript{119} When it comes to big data activities, much of the value of the processed personal data is not evident at the time these datasets are collected and consent is normally given. The previously, relatively ‘simple’, relationship between individuals and data processors is becoming more complex as processors may change and datasets may be combined.\textsuperscript{120} In order to find more effective and easier ways to obtain valid consent of their customers, companies spend increasing amounts of resources to communication with consumers on one hand, and on the other hand to product development to find new means of obtaining consent.\textsuperscript{121}

\textsuperscript{111} See for example Case C-398/15 Salvatore Manni [2017], ECLI:EU:C:2017:197, para. 41.
\textsuperscript{112} Von dem Bussche 2016, p. 580.
\textsuperscript{113} These categories of sensitive personal data provide stronger legal protection for certain sensitive groups, such as children. For the notion of ‘sensitive persona data’, see Case T-190/10 Egan and Hackett [2012], ECLI:EU:T:2012:165, para. 101.
\textsuperscript{114} EC Opinion on the Internet of Things 2014, p. 7.
\textsuperscript{115} Voigt 2017, p. 92-93.
\textsuperscript{116} Ibid., p. 1-2. The right of access (art. 15 GDPR) is an important concept when ensuring data subjects’ control over their persona data (for example Voigt 2017, p. 152-153). See Case C-553/07 Rijkeboer [2009], ECR 1-03889, paragraphs 51-57 and 64-66; Case C-486/12 X [2013], OJ C 45, 15.2.2014, p. 13-14, paragraphs 22, 25, 28-30.
\textsuperscript{117} It is necessary to note that article 7(3) GDPR includes the data subject’s right to withdraw the previously given consent at any time. For the notion of ‘consent’, see Joined Cases C-92/09 and C-93/09 Schecke and Eifert [2010], ECR I-11063, para. 54 and Case C-291/12 Schwartz [2013], ECLI:EU:C:2013:670, para. 32.
\textsuperscript{118} The GDPR enables EU Member States’ national legislation to create or specify legal bases for data processing (Voigt 2017, p. 100-101).
\textsuperscript{119} Hermestrüwer 2017, p. 10. However, as new technologies are emerging, difficulties might occur when ensuring free and informed consent online (Safari 2017, p. 821).
\textsuperscript{120} Cate 2013, p. 67.
\textsuperscript{121} Voigt 2017, p. 242.
Data processing based on consent can be defined as an identification of the data subject’s agreement to the processing of its personal data.\textsuperscript{122} This agreement can be given for example by a clear affirmative action or by a statement (art. 4 No. 11 GDPR). The GDPR states that the controller has the burden of proof for the data subject’s consent (art. 7(1) GDPR).\textsuperscript{123} In other words, it has to be able to demonstrate consent, for example, in a case where the data subject claims not to have given the valid consent required. As the GDPR does not provide formal requirements for obtaining consent, the burden of proof requirement seems to be important especially online.\textsuperscript{124} Online companies might be at risk of being non-compliant with data protection law for different reasons, such as because of a lack of adequate supervision mechanisms.\textsuperscript{125}

As mentioned, the GDPR does not provide rules concerning the formal requirements of the consent. Although some of the national laws of the Member States during the DPD era provided such obligations\textsuperscript{126}, the GDPR allows unambiguous consent given by oral or written means, including electronic measures.\textsuperscript{127} For practical reasons concerning the burden of proof, the written form\textsuperscript{128} is arguably the most advisable. In the future, the possibility to obtain consent by electronic means is likely to gain ground. However, this would probably result in increased administrative burden of data controllers as it could require a separate protocol for the declared electronic consent.\textsuperscript{129}

In order to be legally justified, consent has to be given voluntarily. If the data subject does not have free or genuine choice, consent given is not voluntary.\textsuperscript{130} Thus, it has to be possible to refuse or withdraw consent without hindrance.\textsuperscript{131} In special circumstances, where there exists a clear imbalance between the data subject and the controller, consent may not be used as a justification for data processing activities.\textsuperscript{132} The GDPR also prohibits consent acquired as a condition for the performance of a contract if the personal data in question is not necessary for the contractual performance (art. 7(4) GDPR).\textsuperscript{133} This requirement is likely to affect especially online

\textsuperscript{122} For the scope and elements of the data subject’s consent, see EC Guidelines on Consent 2017, p. 6-17.  
\textsuperscript{123} The requirement of consent is in accordance with the principle of controller’s accountability under art. 5(2) GDPR.  
\textsuperscript{124} Voigt 2017, p. 93. The writer suggests that a double opt-in procedure could be used when obtaining the consent online. The first phase would include the declaration of consent by the data subject. In the second step, a personalized verification email would be sent to the data subject. This procedure could serve as a proof of having obtained the consent for the controller.  
\textsuperscript{125} Monteleone 2015, p. 118.  
\textsuperscript{126} For example, German Data Protection Law requires consent in written form (Voigt 2017, p. 94).  
\textsuperscript{127} Recital 32 GDPR.  
\textsuperscript{128} Von dem Bussche 2016, p. 576, 580. See also recital 32 GDPR. In the online context, the formulation ‘clear and affirmative act’ (art. 4 No. 11 GDPR) of the data subject could indicate for example ticking of an unticked box when visiting a website or any online statement indicating acceptance of the proposed data processing activity.  
\textsuperscript{129} Voigt 2017, p. 94.  
\textsuperscript{130} Recital 42 GDPR.  
\textsuperscript{131} Art. 7(3) GDPR.  
\textsuperscript{132} The risk of imbalance is high for example in cases where the controller is a public authority (rec. 43 GDPR). No other cases are mentioned in the regulation and the identification should take place on a case-by-case basis (Voigt 2017, p. 95). However, according to the EC Guidelines on Consent 2017 (p. 8), the employment context could be a potential one for the imbalance to occur.  
\textsuperscript{133} Recital 43 GDPR. According to Voigt and Van dem Bussche, the scope of this requirement remains unclear and may be targeted only to service providers abusing their monopoly position (Voigt 2017, p. 95).
service providers when gathering personal data. They might have to adjust and review their processes and structures given forthcoming changes, if necessary. The aim of the legislation seems to be the protection of individuals against unfair exploitation of personal data, which is becoming an increasingly valuable business asset for companies.

The consent requirement of the GDPR includes a specific and informed affirmation of the data subject that must be given for the processing of personal data. The data subject should be aware at least of the purposes of the processing of personal data and of the identity of the controller. If personal data are processed for purposes other than those originally consented to, the change will also have to be compatible with the purpose for which the data was initially gathered (art. 6(4) GDPR). The information requirement covers all purposes of processing (granularity). If there are several purposes, the data controller must acquire consent for all of them. It should be noted that consent is not considered freely given, if the affirmation statement does not allow separate consent for different operations. Whether consent is appropriate for an individual data processing activity depends on the context of this separate operation. Nevertheless, if separate data processing operations construct a single service that cannot be divided into several parts, consent separation seems not necessary.

### 2.2.3.2 Other statutory permissions under article 6 GDPR

If data processing activity is not based on consent pursuant to Article 6(1) GDPR, it can be justified based on other statutory permissions under the same article. In order to be considered lawful, also other applicable laws must be respected. For this reason, it is typical that data processing entities preventively obtain the data subject’s consent in order to justify their processing operations. Despite the different legal grounds provided in the GDPR, entities should always seek to obtain the primary legal permission among the available possibilities. As the conditions for obtaining the valid consent or other legal basis for the personal data processing have become stricter and

---

135 Voigt 2017, p. 96. After the GDPR comes into force, the data processing entities should consider limiting ‘unnecessary’ data collection as a violation of art. 7(4) will be punishable with fines of up to 4% of the total annual worldwide turnover or €20 million (art. 83(5) GDPR).
136 Recital 32 GDPR and EC Guidelines on Consent 2017, p. 12-13. For the information requirement of fair processing, see Case C-201/13 Smaranda Bara [2015], ECLI:EU:C:2015:638, paragraphs 34-38.
137 Recital 42 GDPR.
138 Gierschmann 2016, p. 54.
139 See EC Opinion on Consent 2017, p. 11 and recital 32 GDPR.
140 Recital 43 GDPR.
141 Laue 2016, rec. 18.
142 See art. 6(2) and 6(3) GDPR. These statutory permissions include the following: contractual necessity (b), controller’s legal obligation (c), protection of the vital interests of the data subject or another natural person (d), public interest related task or official authority vested in the controller (e) and the legitimate interests of the controller. For the concept of ‘necessity’ under art. 7(e) DPD (art. 6(1)(e) GDPR), see the following cases: Case C-524/06 Huber v Germany [2008], ECR I-09705, paragraphs 50-52; C-70/10 SABAM [2011], ECLI:EU:C:2011:771, paragraphs 50-51 and Case C-615/13 P ClientEarth [2015], ECLI:EU:C:2015:489, paragraphs 51-58.
143 Hacker 2017, p. 9-10 and Kuschewsky 2014, p. 5. These legal permissions are abstractly formulated and are partially subject to national specifications within the EU (Voigt 2017, p. 100).
in many ways more specified, the evaluation and choice of the most suitable legal basis appears to be important.¹⁴⁴

In its judgement C-73/16 Peter Puškár [2017], the CJEU assessed the alleged infringement of personality related rights by the Slovak administrative tax authorities. The claimant sought the removal of his name from an administrative document including names, identification numbers and other personal information as well as the deletion of any reference to his name in the IT systems of the financial authority.¹⁴⁵ When answering to the second question of the Supreme Court of the Slovak Republic, the CJEU analysed the possibility to create a list of personal data for the purposes of tax administration (public authority combating tax fraud) without consent of the data subjects concerned.¹⁴⁶ The Court assessed the question in the light of the Data Protection Directive and the ECFR. As a rule, the data processing activities had to comply and satisfy not only the obligations under the DPD but also the requirements laid down in the articles 7 and 8 of ECFR¹⁴⁷. However, article 7(e) DPD provided an exception under which personal data could be processed in the activities where necessary for the public interest or in the exercise of official authority.

According to the CJEU, the collection of the tax and combating tax fraud fell within the notion of ‘tasks carried out in the public interest’ expressed in article 7(e) DPD. The Court found that the activities of the Slovak tax authorities and the creation of an administrative list without the consent of the data subject could be justified by article 7(e) DPD. However, this required the involvement of public interest and that the list-drawing measures were appropriate and necessary for the purposes and objectives pursued. Thus, the principle of proportionality (art. 52(1) ECFR) also had to be respected.¹⁴⁸ The CJEU stated that also the other conditions for the lawfulness data processing had to be satisfied. This might reflect the growing importance of the general principles of the GDPR and the new compliance challenges data processing entities may be facing in the future. In addition, entities processing personal data should always ensure compliance with the principle of proportionality although they already have a legitimate interest for data processing.

The contractual necessity constructs the second possible legal basis for data processing named in the GDPR.¹⁴⁹ The concept of ‘contract performance’ has to be interpreted in a specific contractual context and is irrespective of the relevant phase of the contract.¹⁵⁰ This justification can only be used if there is a direct link between the

¹⁴⁴ Voigt 2017, p. 101. See also article 5(2) GDPR. The principle of accountability requires that the data controllers can prove the legality of their data processing activities.
¹⁴⁵ Case C-73/16 Peter Puškár [2017], ECLI:EU:C:2017:725, paragraphs 25-29.
¹⁴⁶ Ibid., para. 32.
¹⁴⁷ For the notion of ‘legal person’ protected by articles 7 and 8 ECFR, see the following cases: Joined Cases C-92/09 and C-93/09 Schecke and Eifert [2010], ECR I-11063, para. 53; Case T-198/03 Bank Austria [2006], ECR II-01429, para 95.
¹⁴⁸ Case C-73/16 Peter Puškár [2017], paragraphs 102-117.
¹⁴⁹ Another dimension of the contractual justification concerns the initiation of a contract at the request of the data subject. Because this preparatory context requires the participation of the data subject, the contractual necessity condition could also cover the contractual purposes between the data subject and a third party.
purpose and the activities in question. Processing will be considered necessary if the contract in question cannot be fulfilled without the data processing activities. Another purpose of contractual requirements concerning personal data processing is to limit the overall amount of personal data that can lawfully be modified. For example, many of the IoT devices base their functioning on excessive data processing but, in reality, only some of these data processing activities are necessary for the contractual purpose. For this reason, justification concerning the contractual necessity only applies in limited cases. Moreover, the key element of this justification method seems to be the case-by-case based balancing of the necessity and the relevant contractual provisions of the case.

Lawfulness of personal data processing can also be based on the prevailing legitimate interests of the entity (controller) or a third party in question. Third party interests have a growing importance as many firms are willing to process personal data on behalf of others, such as their clients. The wording of the first phrase of article 6(1) GDPR is relatively vague and contains several unclear notions. The data processing activities shall be considered lawful if the balancing of interests indicates that controller’s interests prevail over the legitimate need to protect data subjects. This test should always include the evaluation of data subject’s reasonable expectations. In addition, the controller is responsible for the burden of proof concerning the legitimate interests. In order to be legitimate, these interests must be assessed on case-by-case basis and they can be for example of economical, legal, social, idealistic or other nature. The regulation recognizes direct marketing purposes as possible basis for legitimate interests of a controller if the balancing test is still in favour of the data controller.

In reality, the data subject’s rights may increasingly overrule the legitimate interest of the controller in the context of data processing operations. The fundamental right to privacy might easily be affected by personal data, when it relates to the state of health, intimacy, location, home or other aspects of the data subject’s private life. For this reason, it seems difficult for the economic operators to justify personal data processing in these circumstances. Justification based on controller’s legitimate interests is a general clause used in cases where the data processing is highly relevant. However, article 6(1) No. 2 GDPR excludes from the material scope of the regulation processing activities carried out by public authorities when carrying out their tasks.

2.3 The challenges of Big Data for the European data protection legislation

One of the main goals of the GDPR is to respond to the growing exploitation of personal data in the digital economy. As a result of fast technological development and

---

152 Ibid., p. 241.
153 Voigt 2017, p. 103-104.
154 Recital 47 GDPR. The notion of direct marketing purposes is not specified in the legislation so it might raise legal concerns in the future. However, Voigt and Van dem Bussche name personalized online marketing to individuals as an example.
globalization in general, new digital business opportunities in the fields of big data, the IoT and cloud computing are emerging. The public interest and the aim of protecting individuals can be seen, for example, in the abstract formulation of many rules of the new regulation. However, it is not completely clear whether the GDPR provides sufficiently specific legal framework for online data processing activities. In the rapidly changing digital environment, the legal rules are at risk of falling short in relation to the dynamics of technological innovation and individual’s online behaviour.

The general aim of the EU privacy and data protection policy is to provide individuals with control rights concerning the various steps of the processing of personal data. In many occasions, the speed of the development linked to big data has still surpassed the understanding of an average consumer. Individuals should be aware of and recognize, at least to some extent, the effects and causal links of their actions. For this reason the harmonization of data protection standards is very important. Exceeding national and sectorial boundaries, inconsistent national law would likely endanger the rights of individual data subjects. This aspect seems to be important especially in the digital age when individuals should increasingly have control over the use of their sensitive information.

To support the assessment of the risks and challenges associated with big data usage, the analysis should be based on the understanding of big data as an approach to data processing rather than regarding it as a specific technique or method. Relying on technological methods of collecting, storing, analysing and extracting value from big data, companies might be able to make better and more efficient business decisions. Big data can also enhance a firm’s ability to gain profitable customer relationships. Considered non-rivalrous, the collection and use of certain piece of data does not restrict other firms from benefitting from it. Despite the business opportunities and other positive economic advantages big data analytics might create, the vast amounts of data are also increasingly used to monitor human behaviour thus creating concerns related to privacy and individual self-determination. The motives of these activities are often related to the predictive surveillance and control potential of big data or consumer profiling activities. The multinational technology company Google and

---

156 Ibid., p. 235.
158 Hemstrüwer 2017, p. 23. See also recital 68 GDPR.
159 Zwitter 2014, p. 1. For example, the lack of transparency of many Internet search engines and the powerless dependency of their users may be problematic (Galindo 2017, p. 10).
160 Kuner 2012, p. 48.
162 Gonçalves 2017, p. 94. For the benefits of big data, see Custers 2016, p. 5-7.
164 Tucker 2014, p. 4. A typical example of the non-rivalrous nature of big data is the use of so-called multi-homing activities where a company or consumer uses multiple providers for the same service (see also Autorité de la concurrence – Bundeskartellamt 2016, p. 28-29).
165 For the discussion, see for example Acquisti 2015A (“Privacy and human behaviour in the age of information”).
166 Sayers 2016, p. 3-6. Data profiling (defined in article 4 No. 4 GDPR) refers to the recording and analysis of a person’s behavioural, psychological and physical characteristics. In the digital economy, companies increasingly seek to benefit from the customer-related advantages and business opportunities that data profiling potentially can create. See also Helberger 2016, p. 3-5. For the risks associated with data profiling, see for example Bevitt 2016.
other Internet companies use big data and consider it a major source of value creation and business asset. For example, Google relies on the data collection from its own services. It uses these datasets not only for operational funding but also to develop and create new search algorithms and other data-intensive digital services. However, securing fair conduct when performing these activities is important also when considering the rights and reasonable expectations of consumers. Because personal data are often integrated into consumer products, many questions stemming from data protection law have become consumer issues and vice versa.

The GDPR is applied to big data sets as soon as they contain personal information. Because of their size and the diversity of content, the potential of personal data to come up through combinations of available information is relatively high. In order to avoid possible breaches and conflicts with data protection legislation, entities might use anonymization or pseudonymization measures and modify the personal information into a form that complies with the GDPR. These methods could help entities to fulfil the organizational requirements set in the GDPR. Nevertheless, as the probability of re-identification of individuals increases, the chances of modifying the data into an anonymous form become smaller.

2.3.1 Compliance with the basic data processing principles

Since many of the rules in EU data protection law are in a relatively abstract form, the significance of the basic principles increases. These rules (art. 5 GDPR) govern all data processing activities falling within the scope of the GDPR. The violation of the principles established in art. 5 GDPR is punishable with severe fines. Especially the principle of accountability seems to be important in the big data context. According to art. 5(2) GDPR, the controller has the responsibility for the compliance of data processing and the burden of proof for the lawfulness of said activities. It is likely that in the future data processing activities will be documented more comprehensively in order to demonstrate compliance with the principles provided in article 5 GDPR.

---

167 Gonçalves 2017, p. 94.
169 Rubinstein 2013, p. 76.
170 For security, compliance, auditing, and data protection in the context of big analytics, see Ohlhorst 2012.
171 Helberger 2017, p. 1428. For example, many companies integrate products, services and persona data collection in one contract (p. 1430). For consumer protection in big data context, see also Sokol 2016, p. 1156-1158, Vladeck 2016 and Helveston 2016.
172 See for example Mantelero 2017B, p. 599-600.
173 Voigt 2017, p. 236-137.
174 The general principles of the GDPR concerning the processing of personal data can be found in the article 5 GDPR (lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability).
175 Article 83 GDPR.
176 The requirements for the security of processing are provided in article 32 GDPR (art. 17 DPD). For the notion of ‘security of processing’, see Case C-342/12 Worten-Equipamentos [2013], ECLI:EU:C:2013:355, paragraphs 24-25 and 28-29.
177 Von dem Bussche 2013, p. 581.
Many big data applications use data from various sources (other applications or operators). Therefore, it may be challenging for data processing entities to determine the scope of data protection with respect to responsibility and liability of their operations. The main rule is that when an entity commissions a data analysis completed by a specialized big data business operator, the commissioning entity (data controller) determines the means and purposes of processing. The controller must choose big data service providers on their ability to ensure adequate data protection standards. However, the roles of the relevant entities should be defined on a case-by-case basis as in practice there might be several entities qualifying as data controllers if deciding on the means and purposes of processing.¹⁷⁸

Compliance with and application of the basic principles of the GDPR may require innovative solutions and considerable efforts from the data processing entities. In particular the principles of purpose limitation, data minimization and transparency (art. 5(1) GDPR) could be challenging without a sufficient level of data protection guaranteed by the organization in charge. Big data activities often include extensive and systematic evaluation of personal information. In order to safeguard the basic principles of lawful processing of personal data, a data protection impact assessment (art. 35 GDPR) might therefore be necessary. It could potentially help to detect the risks and impacts of the planned data processing activities by facilitating the determination of the appropriate safeguard measures to be used and how to comply with the basic principles of lawful data processing.¹⁷⁹

Many companies in the digital economy base their business models on the extensive processing of data in order discover the possible ways to commercially exploit the big data sets available. In this respect, compliance with the principle of transparency (art. 5(1) a GDPR) can be challenging for entities as it requires that data subjects must be informed in a transparent manner of processing activities of the entity in question, if personal data are processed. Articles 13 and 14 GDPR require the data subject is provided with sufficient information of data processing activities prior to the operation (including the identity of the controller, legal basis for and purposes of the processing activity).¹⁸⁰ The principle of purpose limitation (art. 5(1) b) also affects the controller’s informative obligations when processing personal data. Because personal data can only be processed for legitimate, explicit and specified purposes, the processing entity might have to notify several purposes for the use of personal data. It should be noted that the more general the purpose of processing is, the more risk-prone this data processing operation is likely to be and therefore adequate compliance measures have to be taken.¹⁸¹

---

¹⁷⁸ Voigt 2017, p. 237. For the territorial challenges, for example Paez 2016, p. 69-70.
¹⁷⁹ Ibid., p. 236-237.
¹⁸⁰ Rubinstein 2013, p. 75. Empirical studies have shown that individuals do not usually read or understand privacy policies of companies using their personal data. In addition, the terms of privacy often rely on vague language and are easily modified by firms (see for example the complaint of Norwegian Consumer Council, 3.3.2016).
¹⁸¹ Voigt 2017, p. 238.
2.4 The intersection between data protection and competition rules in EU law

New digital business models are often based on acquisition and processing of personal data valuable for companies. Economic competition in digital markets increasingly involves features related to the processing and commercial exploitation of big data. In addition to various economic and business aspects of personal information, the European data protection policy also has a more dignified and human rights oriented dimension.\(^\text{182}\) Hence, it can be argued whether these two relatively different approaches to the collection and processing of personal data are conflicting, or could this regulatory overlap be used to support and strengthen digital markets within the EU. For this reason, it seems to be important to discuss whether there exists an intersection between data protection and competition law in the European legal context.

The common objective of data protection law and competition law\(^\text{183}\) in the EU is to advance market integration and these two legal regimes also share the same concern for the welfare of individuals (in many cases the rights of consumers).\(^\text{184}\) A key goal of data protection policy is the protection of integrity and individual decision-making regarding personal data whereas competition law seeks to provide safeguards against the unlawful exercise of market power. While competition law works largely through negative integration, data protection law is an instrument of positive integration.\(^\text{185}\) Because of different data protection standards within the EU, it is necessary to tackle potential forum shopping strategies as companies might seek to benefit from the most favourable business conditions in countries with narrow data protection regulation.\(^\text{186}\) The prevention of possible abuses of law and related negative effects on competition could also be seen as goals of the GDPR and consequently the territorial scope of its applications remains broad.\(^\text{187}\)

Traditionally, data protection concerns related to personal data have not been seen as a competition law issue.\(^\text{188}\) In its judgement C-238/05 Asnef-Equifax [2006], the CJEU assessed a case concerning a system providing solvency and credit information through the computerised processing of data. These data contained information of the risks undertaken by the participating financial institutions engaged in lending and credit activities.\(^\text{189}\) Concerning the privacy and data protection matters, the Court stated:

\(^{182}\) Costa-Cabral 2017, p. 11.  
\(^{183}\) The competition rules in broad sense usually refer to articles 101-109 TFEU, so in addition to the rules governing antitrust issues, also the rules regulating state aid matters and public undertakings fall within the scope of this concept (Kuoppamäki 2003, p. 21).  
\(^{184}\) Costa-Cabral 2015, p. 11.  
\(^{185}\) Costa-Cabral 2017, p. 21-22.  
\(^{186}\) The creation of a more equal playing field for data protection seems to be important especially for companies whose operations are based in EU Member States with higher regulation standards, such as Germany (Zell 2014, p. 492). See also Roman 2018, p. 2.  
\(^{187}\) Voigt 2017, p. 22. For the extraterritorial nature of data protection, see Van Alsenoy 2015.  
\(^{188}\) Meriani 2017, p. 1.  
\(^{189}\) Case C-238/05 Asnef-Equifax [2006], ECR I-11125, para. 63.
“- - any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection.”

According to Graef, this statement implies that data protection issues should, in principle, be considered separate from competition law, and instead under data protection legislation. However, the relatively flexible wording might open a door to a more parallel application of these two regimes. In other words, the CJEU conclusion does not necessarily mean that data protection concerns do not have relevance in competition law assessment.

According to Ohlhausen and Okuliar, there is a growing consensus that competing firms may try to influence consumer decision-making by offering different levels of privacy for the consumers using their products or services. This aspect is also relevant in the context of the increasingly ‘omnipresent’ Internet of Things and a great deal of focus is therefore put on renewing industry standards in accordance with the technological and data-related changes in the modern interconnected world. Simultaneously, some firms may seek opportunities for joint ventures, mergers or acquisitions in order to acquire new data-advantage possibilities. However, analysis should not be limited solely to privacy concerns. Costa-Cabral and Lynskey argue that the term ‘competition on data protection’ would better describe the multitude of factors regulated by data protection rules of the European Union that influence consumer behaviour. Therefore, one of the main goals of this thesis is also to study, whether personal data are likely to affect firms’ market power and if it potentially influences the decision-making of individuals agreeing to personal data processing.

As a result of the digitalization of data, the scale and possibilities of processing personal data have drastically increased. Personal data are an increasingly valuable asset for companies, and these economic operators are often using considerable financial resources to acquire such data. However, this information often lacks specific price. Instead, acquired datasets can reflect the competitive parameters of

---

190 Ibid., para 63. Commissioner Vestager also referred to this direction when stating that privacy issues should not be confused with competition ones (Margarethe Vestager 17.1.2016).
192 Costa-Cabral 2017, p. 20 and Okuliar 2015, p. 157. For the competitive value of data protection, see Mantelero 2013.
193 Kulwijk 2016, p. 5. The externalities in the multi-sided digital markets often cause winner-takes-all dynamic allowing the most efficient and the most active market players, such as Facebook and Google, to attract the largest number of customers on each side of the market (Hatzopoulos 2017, p. 111 and Thépot 2013, p. 200-205).
195 For the concept of market power, see chapter 3.
196 For example, merger control procedures require assessment of market power resulting from a concentration. In the context of data-driven mergers, many of these cases involve big data and data protection considerations are therefore likely to become increasingly relevant (Costa-Cabral 2017, p. 24). See also Cowen 2016.
197 Murray 2016, p. 5-11 and 51-54.
198 In the EU, the discussion concerning interplay between data protection, competition law and consumer protection was initiated already in 2014 (see EDPS Opinion 2014).
199 For issues concerning access and pricing of raw data and public sector information, see Lundqvist 2015.
quality, innovation and choice to which consumers respond.\textsuperscript{200} In cases like this, the notions of competition on the merits\textsuperscript{201} could reflect the positive effect of corporate rivalry when the less efficient and less attractive firms depart from the market or are marginalized, especially from the point of view of the above-mentioned factors.\textsuperscript{202} Thus, data protection could be seen as an internal influence on substantive competition law assessments.\textsuperscript{203} Data protection law could also serve as an external limit on the enforcement of competition law for example when by precluding the European Commission from accepting certain commitments to undertakings that interfere with the right to data protection.\textsuperscript{204} However, the CJEU has also confirmed that, in particular, article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union limits the actions of EU institutions when they adopt measures that are legally binding.\textsuperscript{205}

Although enforced by separate independent authorities and regulated by different legal rules, the traditional approach might not be up-to-date when considering the special business characteristics and the multitude of private and public interests in the digital economy.\textsuperscript{206} Recent historical amendments to data protection law in Europe also seem to highlight the emerging challenges that stem from technological development, digitalization of business and globalization in general.\textsuperscript{207} According to the GDPR, the private companies and public authorities are able to exploit personal data on an unprecedented scale when pursuing their activities. In order to create and maintain the trust in the existing legal framework, strong and coherent protection and effective enforcement is required in the digital environment.\textsuperscript{208}

The reform of data protection regimes in Europe is likely to have an impact on competition between digital market operators, as the stricter data protection rules will increase their overall administrative burden. As a result, new competition concerns are already emerging.\textsuperscript{209} The extended limits on the collection and processing of personal data might especially affect companies building their services on user data. For this reason, the possibilities to increase revenue through targeted advertising might

\begin{itemize}
  \item \textsuperscript{200} Costa-Cabral 2017, p. 11. The data protection law could potentially provide normative guidance in relation to the non-price competitive parameters that the competition law often seems to be lacking (for example in EC merger procedures) (p. 14). See also Graef 2016A, p. 299-300 and Mandrescu 2017A, p. 6.
  \item \textsuperscript{201} OECD defines this notion by expressing that a dominant enterprise can lawfully engage in a conduct although these activities would lead to the situation where the rivals exit the market or to their discouragement to entry or expansion (see OECD Policy Brief, June 2006, p.1).
  \item \textsuperscript{202} See Case C-209/10 Post Danmark I [2012], ECLI:EU:C:2012:172, paragraphs 22 and 25.
  \item \textsuperscript{203} Costa-Cabral 2017, p. 14. For potential benefits and harms of personal data processing for consumers, see for example Gal 2015, p. 14-44.
  \item \textsuperscript{204} Kuschewsky 2014, p. 20-21. The impact of the right to data protection on competition law has only been assessed in the context of the rights of individual subjects during competition investigation (in some EU Member States, also individuals may face sanctions as a result of a violation of competition rules).
  \item \textsuperscript{205} See for example Joined Cases C-92/09 and C-93/09 Schecke and Eifert [2010], ECR I-09821, paragraphs 85-86.
  \item \textsuperscript{206} See Meriani 2017, p. 2. Recent developments in digital markets indicate that competition concerns might emerge especially in cases involving the use of substantial market power and in market conditions where access to data are essential to firms’ ability to exploit new business opportunities. See chapter 3 and especially Case COMP/M.8228 Facebook/WhatsApp II [2017].
  \item \textsuperscript{207} Meriani 2017, p. 1-2.
  \item \textsuperscript{208} Recitals 6 and 7 GDPR.
  \item \textsuperscript{209} For data-related abuses under article 102 TFEU, see Mandrescu 2017B, p. 8-10.
\end{itemize}
decrease.210 If the new market entrants require access to data in order to compete with the incumbents, the strict rules governing the use and purchasing of personal data could potentially construct entry barriers for new economic operators.211 New provisions on the sale and transfer of personal information could also force companies to collect data organically, reducing the possibilities to a successful market entry of a new firm. In turn, rules permitting only the disclosure and sharing of personal data within a single company might increase the incentives for large market operators to vertically integrate their businesses to circumvent these limits. Therefore, companies are likely to be involved in acquisitions that would otherwise be considered more or less unattractive.212

Naturally, everyone considers monetary aspects of business practices, but it is not always easy to understand the value of personal data in the digital economy where data are often the standard form of currency instead of traditional means of payment.213 For example, data generated by IoT devices can be used to create new business opportunities through the means of smart advertising or smart pricing. They will in turn require price optimization, demand estimation or pattern recognition from data processing entities to meet the demand at the best possible price. In the context of non-price conditions of digital services, measuring the efficiency defences entailing trade-offs214 in mergers cases, acquisitions, joint ventures and horizontal agreements has been proven to be more difficult than in a more traditional environment.215

Due to significant technological developments and the increasing complexity of the digital sector, more than just data processing entities will face considerable challenges when seeking compliance with the new European data protection framework. Moreover, the European regulators and enforcement authorities will have to deal with several, more or less intricate, questions in their efforts to find a balance between different economic, social and moral aspects of law.216

---

211 Brill 2011, p. 18.
212 Graef 2016A, p. 296. See also Lougher 2017, p. 99-100.
213 See Helberger 2017, p. 1428. As personal data are critical ingredients of many smart products and digital services, the concept of “paying with data” has become a popular but relatively inaccurate term.
214 European Competition performs an overall competitive analysis of the effects mergers according to the article 2(1)(b) of the European Merger Regulation (EUMR). For the notion and use of efficiency defence in EU merger control, see for example OECD Roundtable Report 2012 and Szilágyi 2014.
216 The impact assessment of use of personal data on social and ethical values is often more complicated than traditional data protection assessment since these values are more indefinite and context-based (Mantelero 2017, p. 89).
3 ASSESSMENT OF MARKET POWER IN THE DATA-DRIVEN ECONOMY

3.1 Digital business models: important concepts and functionalities

3.1.1 Examples of multi-sided businesses

Although the notion of multi-sided market is relatively novel, multi-sided businesses have existed even before their discovery in economic theory.217 The key characteristic of modern multi-sided businesses (such as online platforms) is the interactions they create between different user groups such as consumers and advertisers. Features related to network effects218 and multi-product pricing form the core of the business practices of online platforms. For example, end-users in a multi-sided market do not always take into account the effects of their actions on the other side of the market. Thus, the interdependency of pricing decisions and the non-internalized network effects among end-users are elements combined in the theory of multi-sidedness.219

Traditional market intermediaries control directly the sale to consumers. However, in the multi-sided markets, especially in the context of e-commerce platforms, these operators delegate this control entirely to the seller by simply determining the affiliation between buyer and seller in a common marketplace.220

Network effects are usually considered either direct or indirect.221 In the context of online platforms, the latter is especially of great importance. The key element in both notions is the rising consumer utility when the number of other consumers purchasing a product increases.222 Whereas the total quality of the product rises directly in case of a direct network effect, an indirect network effect refers to situations where the increase in the number of consumers results in a higher demand for compatible products. Consequently, the value of the relevant product increases in an indirect way.223 In the context of platforms, the growing number of users on an online platform increases the value of this multi-sided platform for the customers on the other side of the market.224 For example, the potential of reaching a larger number of buyers is likely to incline more advertisers to purchase advertising space on Facebook when the number of platform users increase. Due to the aforementioned characteristics, Graef makes a

217 According to Graef (2016, p. 29) the concept of multi-sided market seems to have been first defined by Rochet and Tirole (Rochet 2002, p. 549). See also section 1.4 of the thesis.
218 See for example6, p. 361-363.
221 The economic discussion surrounding network effects was initiated in the mid 1980s (see Shapiro 1985 and 1986). A commonly used example of a direct network effect is a telephone network.
222 Graef 2016A, p. 32.
223 KKV 2017, p. 13. For the general definition of a network effect, see section 1.4 of the thesis.
224 Graef 2016A, p. 33. Alternatively, the term cross-side network effect can be used when describing the strength of one side of the platform affecting the growth of the other side (Weyl 2010, p. 1642).
distinction between ‘ordinary’ indirect network effects and specific ones associated with multi-sided businesses.\(^{225}\)

Many services in multi-sided markets are provided free of charge. This feature may raise questions whether the definition of relevant market is possible if the conditions for monetary compensation are lacking.\(^{226}\) Instead, many of the multi-sided business operators on the “free-side” of the market compete on many non-price related parameters, such as service quality and increasingly on the amount of collected user data.\(^{227}\) Therefore, it seems obvious that the quality and amount of the data resources increasingly determine the competitive strength of companies operating in data-driven markets.\(^{228}\)

### 3.1.1.1 Social networks

Social networks can be defined as online services enabling their users to construct a public or semi-public profile within a limited system, articulating a list of other users with whom to share a connection.\(^{229}\) After the emergence of the first social network sites in the late 1990s, several service providers such as Facebook\(^{230}\), Google+ and Twitter, have attracted millions of users often integrating their daily practices into these services.\(^{231}\) In addition to social networks targeted to the general public, there are specialized social networking services focused on particular user groups.\(^{232}\) When defining the notion of social networks, a distinction should be made between content-oriented and user-oriented online services. The former denotes a network of users determined by a common interest whereas use of the latter type of social networks is characterized by social relationships.\(^{233}\)

The central business model of social network services is to provide interaction and content creation possibilities for their users.\(^{234}\) This feature separates social networks from other advertising-based platforms. The leading social network operators provide their services free of charge and their financing relies mainly on contextual

\(^{225}\) Graef 2016A, p. 33. For this reason, the writer uses the term ‘multi-sided network effect’ in order to make a distinction between these terms.


\(^{227}\) Autorité de la concurrence & Bundeskartellamt 2016, p. 27. See the following cases: Case T-201/04 Microsoft v Commission [2007], ECR II-03601, paragraphs 966-970 and Case T-79/12 Cisco Systems [2013], ECLI:EU:T:2013:635, paragraphs 65-74.

\(^{228}\) Graef 2015A, p. 473.


\(^{230}\) As a proof of the growth of social platforms in popularity, a 2015 study indicated that 71 percent of all the teens in America used Facebook’s social networking services (Stucke 2016, p. 74).

\(^{231}\) Boyd 2008, p. 211. The first website providing social networking services, SixDegrees.com, was launched in 1997. Before the launch of this service, all the key features of social networks existed separately on other websites and were never combined (Graef 2016A, p. 24).

\(^{232}\) Examples of specialized social networking services include Linkedin (professional and business occupations) and ResearchGate (scientist and researchers).


\(^{234}\) See Berendt 2005, p. 5. The writer argues that in a rich interactive environment, the web users are more willing to talk about themselves. Consequently, the increasingly open online behaviour creates a basis for efficient customer relationships for example in the context of e-commerce.
advertising. In turn, online advertisers can analyse the influence of their advertisements on users as consumers by collecting and processing the data created by social networking platforms.

A key feature of targeted advertising on social networking platforms is that service providers are able to sell advertisements including with social context. In addition to user-related advertising, social networks can also cooperate with other platforms. For example, by integrating data generated by social network Google+, the search engine of the same company can display relevant search results for the individual user. Social network providers can improve their service quality by adjusting the relevance of social interactions and suggestions concerning an individual user. Different algorithms are used to study and analyse user behaviour. The willingness to reveal personal information often depends on the level of privacy standards offered to users and the protection against unwanted third-party access. Thus, data collection from the online platform and behavioural user monitoring are essential functionalities of social networking services when companies seek to increase the attractiveness of their network.

3.1.1.2 E-commerce platforms

Since the 1990s, the significance of online environment as a channel for commercial activities has increased together with the rising popularity of the Internet. However, e-commerce practices are still relatively new. The leading e-commerce (electronic trade) platforms such as eBay and Amazon, provide other business operators possibilities to offer their products and services at a fixed price using their platforms. Commercial activities online can be seen falling into three basic categories: trade between companies (business-to-business, B2B), trade between companies and consumers (business-to-consumers, B2C) and trade between consumers (consumer-to-consumer, C2C). As a result of the digitalization of trade, shopping via mobile devices (so-called mobile shopping) is becoming increasingly popular. Consequently, traditional forms of trade are facing challenges, for example falling visitor numbers.

Buyers have free access to most of the e-commerce platforms in the digital market. Some e-commerce dealers limit themselves to specific product or service categories in addition to those who offer a wider range of items. The service providers usually charge sellers different fees for enabling the sale of goods and services on their website.
It may also act as a retailer. However, it has to be noted that advertising services construct only an additional source of revenue for the leading e-commerce platforms.\(^{243}\) As with the Internet in general, e-commerce platforms lower search costs, make consumer information more accessible and facilitate price comparison. The increased number of e-commerce platforms and websites providing aggregated price information tend to increase price competition especially at the retail level.\(^{244}\) An essential characteristic of the e-commerce business models is a specific recommender or recommendation system providing users with purchase suggestions. The total amount of purchases made through the platform is crucial for e-commerce companies as transaction fees are an important part of their revenues. In addition to the collection of data and analysis of purchasing behaviour, the leading e-commerce platform engage in personalized advertising. These activities are based on personal data provided by users.\(^{245}\)

3.1.1.3 Search engines

Search engine businesses have an important function for various user groups such as private website operators, private Internet users and online advertisers. The increasing volume of available online information has led to search engines assuming a key role as an intermediary of information.\(^^{246}\) Since the introduction of the first search engine Archie\(^{247}\), in 1990, the development and commercialization of online search business has been rapid and innovation-driven.\(^{248}\) Search engines are usually classified according to their general (horizontal) and specialized (vertical) nature.\(^{249}\) The latter group differs from the horizontal search engines as it only covers a particular type of content or service provided. The success of the horizontal search engine Google is often credited to the introduction of a specific algorithm (PageRank) ranking search results in relation to their importance, instead of on the basis of the number of their display times on a web page. Today, Google uses the display mode referred to as universal search by merging the different types of search results on their website.\(^{250}\)

The modus operandi of search engine companies such as Google, Yahoo and Bing is based on free user access to the service and financing through contextual advertising. Although end-users are not charged for running queries, this business seems to be

\(^{243}\) Graef 2016A, p. 28.

\(^{244}\) Jozwiak-Gorny 2017, p. 314.

\(^{245}\) Graef 2016A, p. 28-29. For the privacy and data protection issues concerning e-commerce, see Tijmen 2017.

\(^{246}\) Monopolkommission 2015, p. 50 and Stucke 2016, p. 172-173. For the multi-sided nature of search engines, see Hoppner 2015, p. 349-351.

\(^{247}\) The search engine Archie, created by a computer science student at McGill University, was in many ways primitive. Its user interface and search capacity were relatively limited compared to the latest technology (Vanberg 2012, p. 2). See also Devine 2008, p. 67.

\(^{248}\) Vanberg 2012, p. 5.

\(^{249}\) Monopolkommission 2015, p. 51. See also Case COMP/M.5727 – Microsoft/Yahoo [2010], para. 31.

\(^{250}\) Graef 2016A, p. 20-21. In addition to the mainstream companies, alternative search engines are also available. Many of these companies such as DuckDuckGo and Ixquick, emphasize the privacy aspects of users, although they also partly finance their services by selling advertisements.
highly profitable. These platforms sell advertising space and let companies to bid on keywords relevant to their business practices. In other words, the content providing advertisers compete with an untold number of rivals for the attention of users. The advertising model in which the advertiser pays for visits on website and clicks on ads, so-called pay-per-click, is commonly used by search engine platforms. Being free of charge, user data collection appears to be crucial for search services in order to keep attracting both advertisers and individual users. Therefore, the provision of relevant search results, improvements of the search algorithm and other service functionalities of these companies require storage and analysis of user data.

3.2 Definition of relevant market

When assessing possible breaches of EU competition law, the economic concept of ‘relevant market’ becomes central. Considered an analytical tool assisting the detection and assessment of possible competitive constraints in the market, it facilitates the determination of the existence and possession of market power by a firm or firms. By nature, the notion of relevant market is twofold. The adequate market evaluation requires analysis of both product and geographical dimensions of the market. However, it has to be noted that the prevailing definition of relevant market does not take into account potential competitors.

---

251 Search engine companies primarily compete on service quality. Relevant quality indicators include for example the speed of service and the design of the user interface (Monopolkommission 2015, p. 50-51). See also EC Case Comp/M.5727 - Microsoft/Yahoo [2010], para. 101.
252 Monopolkommission 2015, p. 51 and Graef 2016A, p. 22. The sponsored advertisements (sponsored results) are usually separated from the non-sponsored (organic) results. To find, index and display the latter group, search engines use specific software applications (web crawlers, spiders or robots). For the definition of a web crawler, see EC Comp/M.6281b – Microsoft/Skype [2011], footnote 10.
253 Graef 2016A, p. 23. As stated in section 2.4 of the thesis, the service quality, in particular the relevance and personalization of search results can serve as non-price competitive parameters.
254 The term antitrust market is used as an alternative to the notion of relevant market. However, with this concept the European Commission refers to areas of competition law other than mergers (Jones 2016, p. 56).
255 For the definition, see particularly the EC notice on the definition of relevant market (1997). According to the document, the main sources of The Notice introduced the ‘hypothetical monopolist’ test (SSNIP test) to facilitate the definition of relevant market (paragraphs 115-119).
256 According to the EC Notice, the main sources of competitive constraints in the market are the following: demand substitutability, supply substitutability and potential competition (para. 13). For the special case of 'one-way-substitutability’, see Case T-340/03 France Télécom [2007], ECR II-107, paragraphs 88-90.
257 Defining the relevant market is considered necessary at least in the following circumstances: consideration of the appreciable effect of an agreement restricting or substantially eliminating competition or effect on trade between Member States under article 101 TFEU; requirement of a market share test included in the block exemption regulations; consideration of the dominant position of an undertaking under article 102 TFEU; determination of the possible significant impediment effects on competition under the EUMR, especially when strengthening a dominant position (Whish 2015, p. 29).
258 According to the Oxford English Dictionary (online version), market refers to a geographical area of commercial activity including the potential demand for a specific commodity or service provided by such area. In addition, this definition covers the potential demand for a service or commodity within a demographic group and the commercial activity of such a group in total (frequently with the area or group specified).
259 Whish 2015, p. 28-29 and ICN Recommended practices for Merger Analysis, part III. For the notion of market power in the digital environment and in general, see section 3.3.
In the previous years, the EU competition authorities and the CJEU have received critique for too one-sided focus on price, characteristics and use of the products in their assessment. In reality, these parameters might not sufficiently reflect the relevant features of the market. There is a risk of too much subjectivity being involved in the assessment if the relevant market is not defined scientifically. Despite possible shortcomings or general critique, the definition of relevant market plays a central role when evaluating the exercise of market power.

The CJEU has confirmed that the definition of the relevant market is different depending on whether the article 101 TFEU or 102 TFEU is applied. The purposes of article 102 TFEU require this definition as a precondition for all the cases including alleged anti-competitive behaviour. This results from the fact that the determination of the existence of a dominant operator requires preconditionally the definition of the relevant market. The assessment of article 101 TFEU in turn requires the analysis of relevant markets when determining if an agreement, decision or concerted practice has the potential to have an impact on the trade between Member States by restricting, preventing or distorting competition in the market.

3.2.1 The relevant product market

The relevant product market can be understood encompassing all products or services regarded as substitutes on the basis of their prices, characteristics and intended use. Already in 1973, the Court of Justice of the European Communities held that this definition was of great importance. The assessment of the case law of the CJEU expanding to several decades shows that the essential element in the market definition is the interchangeability (substitutability) of competing products. In its judgement C-179/16 Hoffmann [2018] concerning the artificial differentiation between the medicinal products of two competing firms, the CJEU stated that the effective competition in the relevant product market required a sufficient degree of

---

260 Jones 2016, p. 64.
261 Kaplow 2011, p. 437.
262 Whish 2015, p. 43.
264 EC Notice on the definition of relevant market, para. 7. This notion has been approved by the EU Courts. See for example Case 85/76 Hoffmann-Laroche [1979], ECR 461, para. 28; Case T-446/05 P Amann & Söhne [2010], ECR II-1255, para. 55 and T-427/08 CEHR [2009], ECR II-05865, paragraphs 68-70.
265 Case 6-72 Continental Can [1973], ECR 1973-00215, para 32. In the judgement, the Court held that the delimitation of a relevant product market was crucial when identifying a dominant position. The importance to the application of Merger Regulation can be seen in the Case T-62/98 Volkswagen [2002], ECR II-2707, para. 231.
266 See for example Jones 2016, p. 63. See also Case C-1/12 OTOC [2013], ECLI:EU:C:2013:127, paragraphs 75-77 and Case 27/76 United Brands [1978], ECR 00207, para. 22. According to Blair, the substitutability of the demand side of the relevant market consist of three main elements: identical products, products that are regarded as the same product by consumers in spite of certain negligible physical or brand differences as well as other products considered close substitutes (Blair 1998, p. 7).
interchangeability between all the products and services forming part of the same market.\textsuperscript{267} The assessment of interchangeability usually focuses on the customer perspective (demand side). In some cases, it might be meaningful to also consider the substitutability of supply side of the market as well.\textsuperscript{268} However, measuring this concept can be challenging and many of the problems concern the lack of or unreliability of available market data. Partly for these reasons, the CJEU has acknowledged the margin of assessment of the European Commission in economic analysis related to competition enforcement.\textsuperscript{269} In practice, the Commission tends to define several possible and alternative relevant markets. If no competitive constraints are detected, the assessment procedure will be ended.\textsuperscript{270}

When assessing the possible abuse of dominant position (art. 102 TFEU), the number of relevant markets is usually smaller, depending on the scope of the effects of the alleged abusive market behaviour.\textsuperscript{271} In contrast, merger procedures and impact assessments under the EUMR may often require more elaborate and case-by-case assessment as the merging companies are often operating in several different markets.\textsuperscript{272} It is important to understand, that this assessment is always completed by reference to the facts prevailing at the time, and not by the present circumstances.\textsuperscript{273} The European Commission routinely contacts competitors and customers in cases requiring market definition and the SSNIP test is often applied. In addition measures such as marketing studies, consumer surveys, quantitative tests and substitution evidence from the recent past are used when defining the product market.\textsuperscript{274}

### 3.2.2 The relevant geographic market

The significance of relevant geographic market increases as the European Single Market expands to new business environments.\textsuperscript{275} According to the EC study, the

\textsuperscript{267} Case C-179/16 Hoffmann [2018], ECLI:EU:C:2018:25, paragraphs 50-52. Traditionally, similar products are assumed to compete more fiercely against one another than dissimilar products (Stucke 2016, 129).

\textsuperscript{268} For the supply-side substitutability, see the following cases: Case C-52/92 P Hilti [1994], ECR I-667; T-301/04 Clearstream [2009], ECR II-3155, paragraphs 58-60; Case T-219/99 British Airways v Commission [2003], ECR II-5917, para 91.

\textsuperscript{269} However, the CJEU has the final word when assessing the accuracy and reliability of the EC’s evidence (Whish 2015, p. 31). See also Case T-201/04 Microsoft v Commission [2007], ECR II-03601, paragraphs 87-89 and Case T-321/05 AstraZeneca [2010], ECR II-02805, para. 32.

\textsuperscript{270} See for example Case COMP/M.7217 Facebook/WhatsApp I [2014], p. 3-14.

\textsuperscript{271} In several decisions, the CJEU has held that products such as consumables and spare parts form a separate market from the end-products for which they are necessary. However the distinction is not always clear (Whish 2015, p. 38). See for example the following cases: Case 238/87 Volvo v Veng [1988], ECR 6211 and Case 53/87 Renault [1988], ECR 6039 (spare parts); Case C-333/94 P Tetra Pak [1996], ECR I-5951 (consumables); Case C-56/12 EFIM [2013], OJ C 344, 23.11.2013, p. 20-20 (printers and ink-jet cartridges).


\textsuperscript{273} The General Court of the EU has confirmed this interpretation in its Coca-Cola -judgement (Joined Cases T-125/97 and T-127/97 Coca-Cola [2000], ECR II-01733, para. 82.

\textsuperscript{274} EC Notice on the definition of relevant market (1997), paragraphs 35-43.

\textsuperscript{275} See O’Donoghue 2013, p. 128-130. Traditionally, in the decisional practice of the EU Courts and the Commission, four types of geographic market definitions have been found: Worldwide markets, EU-wide markets, national markets and local markets.
analysis of merger decisions since 2003 reflects the fact that the Commission is increasingly focusing on wider geographic markets. In some cases, the area of market supply is relatively narrow for legal, technical or other reasons. However, if the geographic scope of the relevant market is broad such as in many digital markets, it may have a great impact on the assessment of an individual case.

In its early judgement 27/76 United Brands [1978], the CJEU held that when assessing the competitive conditions under article 102 TFEU, the evaluation of the economic power of the undertaking required a clearly defined and sufficiently homogenous geographic area in which the product is marketed. Evidence used by the European Commission in the assessment of geographical market conditions include for example basic demand characteristics, trade flow and patterns of shipments as well as current geographic pattern of purchases.

The definition of relevant geographic market has been important especially in cases where the determination of dominance has been central issue in the assessment of the Court. In certain specific cases, the definition of temporal market might also be of great importance. If market conditions are changing rapidly, a company might only face competition irregularly. Conditions such as weather might influence the business practices of a company. In the AstraZeneca judgement [2010], the CJEU analysed the competitive interaction of two rival companies over the whole period of the alleged abusive behaviour of the other firm. It confirmed the previous decision of the General Court stating that the gradual increase in the uses of one pharmaceutical product at the expense of a competing product was insufficient for concluding the two products being part of the same market.

### 3.2.3 Defining the relevant market for personal data

The traditional starting point for the definition of relevant market is to base the assessment on the products or services offered in the market. However, in the context of multi-sided platforms an alternative approach would be to analyse the relevant market in relation to the financing of the service provider. In the digital business environment, this aspect would signify the importance of advertising as the basis for many online intermediaries. In other words, the relevant market would then consist of

---

276 EC Competition policy brief 3/2015. According to the study, 61% of EC merger decisions included assessments of markets EEA wide or wider in scope, compared to the 48 % share ten years ago (p. 2).
277 See Whish 2015, p. 40. For business practices, challenges such as transportation costs or legal barriers might reduce the size of the relevant geographical market. In the latter case, the rules protecting the free movement of goods (art. 34-36 TFEU) or services (art. 56-62 TFEU) might be applied.
278 See Case COMP/M.1672 Volvo/Scania [2000].
280 Whish 2015, p. 41-42.
281 See for example the following cases: Case 247/86 Alsatel [1988], ECR 1988-05987; Case T-151/05 NVV [1988], ECR II-01219; Case T-57/01 Solvay [2009], ECR II-4621, paragraphs 239-260.
282 Whish 2015, p. 42. See the following cases: Case 27/76 United Brands [1978], ECR 207 and Case 77/77 BP v Commission [1978], ECR 1513.
283 Case C-457/10 P AstraZeneca [2012], ECLI:EU:C:2012:770, paragraphs 36-51.
a *market for personal data* monetised through online advertising. In contrast to traditional ICT companies selling their technology to consumers, many platforms gain their business profits by exploiting the valuable data collected from their users. Currently, the definition of market for data is only possible when the data are traded in the market. According to the main principles of competition law, data cannot be an object of the relevant market unless *economic transactions* take place between users and providers of data. Additionally, the online platform service providers are not allowed to trade or sell data to third parties.

Since the current competition law standards for defining the relevant market demand the existence of *supply and demand* for the product or service, it is not completely clear whether the collection and processing of personal data by the platform operator could qualify as an *economic exchange*. Contrary to possible arguments concerning the increased awareness of consumers, Graef argues that the provision of personal information for the purposes of the search or social networking functionalities would not be likely to constitute a genuine supply of a product by the platform users. If considered *suppliers of data*, users would neither be able to determine the *amount and quality* of personal data they are willing to supply nor to negotiate the conditions of possible counter-performance. With opaque data processing practices and *take-it-or-leave-it* -style online marketing, the competitive market seems to be lacking an optimal level of individual control over personal data. Thus, unilateral decision-making over the use of personal information by platform service providers and the characteristics of current interaction in the online business environment seem to constitute rather a one-sided retrieval than an economic transaction.

### 3.3 Definition of market power

#### 3.3.1 Conceptual issues and methods of assessment

An essential element of the functioning of a free market is competition between economic operators. At the heart of competition law regulation is the objective to

---

284 Graef 2016A, p. 87. In the US Google/DoubleClick merger case (2007), the Federal Trade Commissioner Harbour suggested to define a market for data. It would be separate and apart from the service markets of the merging parties (FTC 2007, p. 9).
286 Graef, 2016A, p. 88. Examples of economic transactions involving data include Twitter’s data licensing activities and the sale of the collected consumer data. These data sets are sold to other businesses by data brokers.
287 EC Notice on the definition of relevant market (2007), paragraphs 13-23.
288 See for example Casadesus-Masanell, 2013, p. 25-26. The writers assume that consumers are aware of the disclosure practices of the online service providers and internalize the impacts on their usage and decisions of services.
289 For an overview of the challenges of users’ privacy awareness, see Tsohou 2017, p. 440-442.
290 Graef 2016A, p. 87. According to Graef, these factors would not seem to constitute adequate indicators for market power because different data sets of service providers cannot be easily compared. However, factual information (age, occupation etc.) will normally have lower value than information indicating the behaviour of a specific user (Graef 2016A, p. 260).
292 Graef 2016A, p. 87.
protect this competition by regulating and controlling the exercise of market power.\textsuperscript{293} Being one of key concepts in the economic approach to competition law, market power can be defined as the ability of a company to raise market prices of products or services over the competitive level for a certain period of time in order to gain economic profits.\textsuperscript{294} A company having a high degree of market power or a dominant position is not ipso facto problematic as long as it does not abuse this position at the expense of the competitors and consumers.\textsuperscript{295} However, the use of substantial market power, by a single firm or several firms together, usually results in lower quality, higher prices and less innovation in the market for products and services.\textsuperscript{296} With a substantial degree of market power, these unilateral activities can be carried out without the risk of losing the market to competitors as a result of the unprofitable price increase.\textsuperscript{297}

In individual cases, the estimation and measurement of market power requires expert judgement to assess the degree of dominance on case-by-case basis.\textsuperscript{298} This delimitation is necessary in order to determine whether the companies with significant market power should be subject to article 102 TFEU regulating the abuse of dominant position.\textsuperscript{299} If a firm only has a marginal degree of market power in the relevant market, it is not likely that a unilateral conduct of this economic operator would have negative effects on consumer welfare or other protected interests. In other words, firm dominance can be seen as a type of filter allowing the competition authorities to focus only on the cases most potentially harmful to competition.\textsuperscript{300} As competition authorities have taken measures in order to harmonize the assessment practices concerning significant market power (dominance) and a relatively broad economic consensus about the relevant factors prevails, this dimension of competition enforcement has been relatively uncontroversial.\textsuperscript{301} However, the characteristics of digital markets often differ from traditional market conditions. Hence, the rise of new digital business models is likely to raise concerns about the need for new approaches.\textsuperscript{302}

When determining a firm’s market power, two prevailing methods are used. The most commonly used approach is the indirect method.\textsuperscript{303} It involves a structural approach consisting of the following three phases: the definition of a relevant market, assessment of the market power of the firm or firms and the so-called barriers to entry

\begin{footnotesize}
\textsuperscript{293} For the establishment of dominant position, for example Ortiz Blanco 2011, p. 46-65.
\textsuperscript{295} Vanberg 2017, p. 7. This conclusion can also be derived from the Finnish Competition Act, since Section 7 only prohibits the abuse of dominant position. However, in its early decision 322/81 Michelin I [1983], ECR 03461, the CJEU stated that a company in a dominant position has a 'special responsibility not to allow its conduct to impair undistorted competition' on the internal market (para. 57).
\textsuperscript{296} Jones 2016 p. 2. Prices, quality of goods and services, and innovation are examples of competitive parameters.
\textsuperscript{297} Posner 1980, p. 937.
\textsuperscript{298} For the measurement of significant market power, see for example Monti 2006, p. 34-38 and Lerner A. P. 1934.
\textsuperscript{299} See for example, Kuoppamäki 2012, p. 1096.
\textsuperscript{300} Coscelli 2013, p. 353.
\textsuperscript{301} Coscelli 2013, p. 383.
\textsuperscript{302} The definition of relevant market and assessment of market power of online platforms is further discussed in chapter 4.
\textsuperscript{303} For example, the European Commission uses the indirect method and this approach also has the approval of the European Court of Justice (Jones 2016, p. 55).
\end{footnotesize}
analysis. The third element is an essential factor in the profit-maximization strategy of a company using significant market power as the barriers of entry facilitate the efforts of keeping competitors from entering the market. The direct method utilizes econometric analysis, dealing especially with residual demand curves of the companies operating in the market. However, the application of statistical methods in empirical market analysis requires data, which are often difficult to acquire or are not available at all.

Although not explicitly included in the article 102 TFEU, the economist’s definition of substantial or significant market power is generally considered synonymous with dominance. They are also used interchangeably in the European economic law in general. The following three central dimensions in the assessment of market power are summarized in the European Commission’s Guidance on Article 102 TFEU Guidance Priorities:

- constraints imposed by the existing supplies from, and the position on the market of, actual competitors (the market position of the dominant undertaking and its competitors),

- constraints imposed by the credible threat of future expansion by actual competitors or entry by potential competitors (expansion and entry),

- constraints imposed by the bargaining strength of the undertaking’s customers (countervailing buyer power)

Despite the fact that most companies do have a certain degree of market power when measured in the short term, it is the substantial and often abusive behaviour of a firm possessing market power over a longer period that is likely to raise competition concerns. In the assessment of market power, market shares have traditionally provided useful information of the market structure and conditions as well as of the relative importance of different economic operators in the market. This aspect is usually the first step in the estimation of a firm’s market power. For example, when assessing the anti-competitive effects of an agreement between undertakings, the

---

304 Coscelli and Edwards note that instead of finding the dominance or substantial market power on the basis of a single factor, the European Commission generally undertakes a ‘comprehensive survey’ approach including quantitative assessment of market structure, qualitative assessment of market characteristics and direct assessment of prices or profits (Coscelli 2013, p. 355).

305 Jones 2016, p. 54-55. For a more economic approach (industrial organization) to the direct method, see Carlton 2005, p. 66-99.

306 See for example Case 85/76 Hoffman-La Roche [1979], ECR 461, para. 38. According to Jones and Suffrin, the European Commission has not issued a general Notice on market power that would be analogous to the Notice on the definition on the relevant market (Jones 2016, p. 320). See also Korah 2017, p. 397-399.

307 Coscelli 2013, p. 352. See also Hay 1992, p. 817-818. According to Hay the terms market power and monopoly power are also used interchangeably.

308 EC Guidance on Article 102 TFEU Enforcement Priorities, EUVL C 45, 24.2.2009, s. 7-20, para. 12. These matters are also identified in the EC Guidelines on the application of Article 101(3) TFEU, EUVL C 101, 27.4.2004, s. 97-118.

309 Due to the delimitations of the study, the concept of countervailing buyer power is not further discussed in the thesis.

310 Jones 2016, p. 54.

311 For an overview of market shares as market power indicators, see Whish 2015, p. 47-51.

312 EC Guidance on Article 102 TFEU Enforcement Priorities, para. 13.
degree of the market share often serves as a proxy, although this figure may be lower in order to article 101(1) TFEU to be applied than in the assessment of dominant position in accordance with article 102 TFEU. However, as previously discussed in the section 3.2, defining the relevant market in the context of potential competition and countervailing buyer power is often problematic. For this reason, it seems clear that also the use of market shares when assessing the influence of potential competition on the existing competitors might be lacking the sufficiently forward-looking analytical approach.

3.3.1.1 Actual competitors

When assessing the dominant position of an undertaking, the principal research question is usually related to the degree of market power the undertaking holds. In the case of statutory monopolies, there is only one economic operator in the market due to a legal provision or statute. As a rule, the CJEU has rejected the arguments concerning the immunity of these privileges from the application of article 102 TFEU. However, as pure monopolies rarely exist, this evaluation is usually focused on the actual competitors of this undertaking.

The market shares often provide important indicative assistance when assessing the market power of an undertaking. According the EC Guidance on Article 102 TFEU Guidance Priorities, they may serve as useful first indication of the relative importance of the economic operators in the market as well as of the structural market characteristics. The market conditions included in this assessment and to which the Guidance refers, also include the degree of product differentiation, market dynamics as well as the development and trend of market shares over time. The probability of the existence of dominance tends to rise together with the size of a firm’s market share. Nevertheless, it is not infeasible that a company has a significantly large market share.

Already in its early judgement C 85/76 Hoffmann-La Roche [1979], the CJEU had indicated that a large market share could in itself be a sign of firm dominance in a

---

313 For example, in order to delimit the application of the prohibition under article 101(1) TFEU, some categories of agreements between undertakings with market shares below certain thresholds are exempted with block exemption regulations. A safe harbour denotes conditions under which the market share is under the thresholds (Jones 2016, p. 56). See for example Commission Regulation 330/2010 (vertical agreements and concerted practices) and Commission Regulation 316/2014 (technology transfer agreements).

314 In the markets with high technology intensity such as many online platform markets, a high market share does not directly indicate the existence of substantial market power (Vanberg 2017, p. 7).

315 Whish 2015, p. 44.

316 Ibid., p. 191.

317 See for example: Case C-T-229/94 Deutsche Bahn [1997], ECR II-1689, para. 57 and Case C-351/12 OSA [2014], OJ C 295, 29.9.2012, p. 21-22, para. 86. If a company has a statutory monopoly, the only special privilege granting immunity is article 106(2) TFEU.

318 For the economic concept and characteristics of a monopoly, see Varian 2010, p. 439-458.

319 Whish 2015, p.

320 Whish 2015, p. 192.

321 A market share of 100 percent is a relatively rare phenomenon. See Case T-139/98 AAMS [2001], ECR II-34113, para 52, where the firm under scrutiny, AAMS, held a de facto monopoly of the cigarette wholesale distribution market in Italy. See also Case T-336/07 Telefonica [2012], ECLI:EU:T:2012:172.

specific market. Later, in the landmark judgement C-62/86 AKZO [1991], the Court formulated a more precise market share indication when clarifying the obligations related to the pricing practices of dominant companies. Starting with a reference to the earlier Hoffmann-La Roche judgement, it stated that a market share of 50 per cent could be regarded large enough to draw a conclusion that without exceptional circumstances the undertaking holding such market share will be considered dominant. This is a clear indication for companies holding large market shares but still falling short from being considered monopolists.

If the market share of an undertaking does not exceed the 50 per cent, it is still possible to find this economic operator to be dominant. In the United Brands judgement, all the factors affecting the firm’s market power were taken into account and consequently a company with the market share between 40 and 45 per cent could be found dominant. Considering the complexity of different market share thresholds and their interpretation, it has been suggested whether there should be a safe harbour limit for market shares, below which a firm could not be dominant.

It is important to notice, that in many cases also the rivals’ market shares shall be taken into account. In its decisional practice, the European Commission has found that if the market share of the next largest competitor of the dominant firm exceeds 20%, there is a great likelihood of dominance. However, this conclusion requires that the shares have remained stable for a significant period of time. The assessment of the rivals’ market position does not solely focus on the individual numbers, but it also includes the cumulative share values in order to determine whether the collective market power potentially affects the firm under investigation to act independently. In the judgement T-219/99 British Airways v Commission [2003], there was found to be a substantial gap between the market shares of British Airways, its closest rival as well as of its five main competitors. The differences in market share were considered sufficiently substantial for the finding of dominance.

---

323 Case 85/76 Hoffmann-LaRoche [1979], ECR 461, para. 41.
324 Case C-62/86 AKZO [1991], ECR I-03359, para. 60. Critics have argued that the presumption in AKZO should be even higher as it has often been applied in too aggressive manner (for example O’Donoghue 2013, p. 147).
325 Whish 2015, p. 193. The EC Guidance on Article 102 Enforcement priorities does not refer to the AKZO presumption. However, it states that the larger market share and the longer period of time during which the market share might serve as preliminary indicators of a dominant position (para. 15). However, all the relevant factors are included in the Commission’s assessment of dominance.
326 Case 27/76 United Brands [1978], ECR 00207, paragraphs 105-107. Nevertheless, market shares below 40% have not usually supported the finding of dominance (O’Donoghue 2013, p. 149). See Case T-219/99 British Airways v Commission [2003], where the General Court held that, in the circumstances of the case, a market share of 39.7% could be regarded as significant (para. 211).
327 Ibid. para. 228.
328 Whish 2015, p. 194. The EC Guidance on Article 102 Enforcement priorities only states that market shares under 40% are ‘not likely’ to indicate firm dominance (para. 14). See also Kuoppamäki 2008, p. 1091-1095.
331 Case T-219/99 British Airways v Commission [2003], ECR II-5917, paragraphs 224-225. Nonetheless, O’Donoghue and Padilla argue that the key element of the assessment of rivals’ market shares is their...
3.3.1.2 Potential competition and barriers of entry

When assessing the potential competitive pressure that a firm with significant market power is facing, market shares may not serve as an effective indicator of market power. The EC Guidance emphasizes to some extent these aspects related to the entry of potential competitors in the assessment of the dominance of an undertaking. In some cases, there might be legal barriers to market entry of potential competitors. For example, intellectual property rights, depending on their duration and strength, may constitute competitive constraints. Other legal barriers include statutory monopolies, tariffs and non-tariff barriers as well as planning regulations and licensing requirements.

Entry barriers of competition can be defined as factors that prevent or hinder firms from entering a specific market. In many cases, these competitive constraints may result from different structural characteristics of the relevant market. When discussing the possible barriers to entry or expansion for potential competitors, several economic advantages have also been identified. For example, if an incumbent undertaking controls an essential facility it is likely to have an economic advantage in the market in relation to its competitors. In addition, the switching costs for consumers changing the supplier or service provider as well as the actual conduct of an undertaking are taken into account when determining the possible dominant position of an economic operator. However, different arguments have been presented concerning the scope of this concept.

When determining whether the behaviour of an undertaking is independent from its competitors, customers and consumers especially in new economy industries, such as online intermediary industry, competition authorities should not rely solely on market shares. Therefore, the evaluation of potential competition is a crucial part of this assessment process. Unlike in traditional markets where competition is linked to price and output, competition in the new economy is characterized by subsequent competitors overturning the market structure as they compete with each other. In this context, it is important to consider the potential to rapidly increase production to meet demand. This is why the importance of rivals’ market shares should not be overstated.

The concept of new economy reflects the change to service-based economy from traditional manufacturing businesses. The three main markets in the new economy include computer software, internet-based businesses and communications services (supporting the first two markets). Lacking the common market features such as stable market conditions, major capital investments, economies of scale, moderate rates of innovation and infrequent entry and exit, the key characteristic of new economy businesses is intellectual property as the principal output rather than physical goods.
case, the market leader\textsuperscript{341} can be under constant competitive pressure if the entry barriers are low and new competitors have the potential to challenge its market power. Hence, identification of potential competitive advantages of the incumbent seems to be crucial as the special features of, for example, online platform industries can give rise to entry barriers reducing the potential competition in the market.\textsuperscript{342}

In the decisional practice of the European Commission and the CJEU, the potential barriers to entry in the technology sector have been discussed in several cases.\textsuperscript{343} In the early Microsoft decision of the European Commission\textsuperscript{344} concerning technological entry barriers, upheld by the General Court\textsuperscript{345}, Microsoft had refused to license interoperability information tied its Windows operating system to the Media Player software of the same company. Also in the later Microsoft (tying) decision, the Commission held that Microsoft could exploit the indirect network effects in the PC operating system market dominated by Microsoft.\textsuperscript{346}

The nature of technological entry barriers found in the earlier competition cases may often be somewhat different from the most recent trends concerning digital business models, such as search engines, e-commerce and social networks. Instead of technological tying and blocking, entry barriers found in online platforms industry seem to have more of an informational character.\textsuperscript{347} With a good reason, it could be argued that the exclusive control over data could enable a dominant company to control user data, effectively leading to insurmountable barriers to entry.\textsuperscript{348} If the incumbent platform can control the qualitative and quantitative accumulation of user-related big data, it could possibly block the potential competitors from the market.\textsuperscript{349} Thus, considering the diminishing returns to scale of the platform industry, one could argue that large data volumes may give a competitive advantage to the market leader assuming that the benefits of extra information start to diminish only when the data quantities are significantly high.\textsuperscript{350}

\textbf{3.3.2 Personal data as a source of market power}

Despite the importance and clarifying aim of the European Commission’s Notice on the definition of relevant market, it does not effectively resolve the problem concerning the role of potential competition in highly dynamic markets such as multi-sided business environment. Dynamic competition is an essential feature of these digital businesses as

\textsuperscript{341} The company or brand having the largest share of the market for a particular product or service (Oxford English Dictionary, online version).
\textsuperscript{342} Graef 2016A, p. 125.
\textsuperscript{343} For cases related to different entry barriers, see for example the following: Case T-342/07 Ryanair v Commission [2010], ECR II-03457; Case C-373/14 P Toshiba [2016], ECLI:EU:C:2016:26; Case T-67/98 Van den Bergh Foods [2003], ECR II-04653 and Case T-472/13 Lundbeck [2016], ECLI:EU:T:2016:449, Case COMP/C-3/37.792 Microsoft [2004].
\textsuperscript{344} Case T-201/04 Microsoft v Commission [2007], ECR II-03601.
\textsuperscript{345} Case COMP/C-3/39.530 Microsoft (tying) [2009].
\textsuperscript{346} Butts 2010, p. 290-291.
\textsuperscript{347} Schepp 2016 p. 121. See also Newman, A 2014B, p. 401-454.
\textsuperscript{348} Graef 2016A, p. 60.
\textsuperscript{349} Shelanski 2013, p. 1681.
the innovative potential of many online platforms is significant.\textsuperscript{351} In addition, these services are often free to at least one of their user groups. For this reason, many traditional economic tools for competition policy analysis, such as the SSNIP test and purely static models of competition, cannot be applied without significant modifications.\textsuperscript{352} The Notice states that when defining the relevant market, competitive constraints resulting from potential competition should not be included in the assessment.\textsuperscript{353} This is somewhat contradictory since the EU Horizontal Guidelines recognise that in certain cases the assessment of competitive conditions cannot be sufficiently based on existing markets.\textsuperscript{354}

In the new economy, multi-sided businesses such as online platforms are usually involved in constant innovative activities as they seek to gain competitive advantages over their rivals. In this respect, the concept of disruptive innovation\textsuperscript{355} could describe the nature of these, often aggressive, business practices.\textsuperscript{356} The prevailing digital business models are based increasingly on innovation and intellectual property is their primary industrial output. If potential competitors are likely to be dependent on the resources and capabilities necessary for the innovative activities of a company, the concept of specialized assets\textsuperscript{357} might become increasingly important.\textsuperscript{358} Since many increasingly significant oligopolistic online markets have emerged in the recent years, one should consider the possibility of defining an additional relevant market for data, to support the competition enforcement efforts and the definition of a relevant market.\textsuperscript{359}

By considering data as a specialized asset in accordance with the EC Horizontal Guidelines, it could be possible to define a potential or hypothetical market in addition to the actual relevant market definition based on services provided to advertisers and users. This approach to the market definition and measurement of market power could serve as a supplementary method when considering the shortcomings of the traditional market share analysis.\textsuperscript{360} Market shares may not be effective indicators when the markets are characterized by technological change or rapid growth.\textsuperscript{361} Generally, multi-

\begin{itemize}
\item \textsuperscript{351}Graef 2016A, p. 585.
\item \textsuperscript{352}Evans 2016, p. 3.
\item \textsuperscript{353}EC Notice on the definition of relevant market (1997), paragraphs 13 and 24.
\item \textsuperscript{354}EC Horizontal Guidelines 2011, para. 304. According to Graef, these assets refer to resources to which potential competitors need access in order to compete with the incumbent.
\item \textsuperscript{355}See for example Cortez 2014, p 182-183. Disruptive innovation refers to innovative technologies departing fundamentally from the existing ones. Being more accessible, less expensive and less complicated, disruptive innovation as a business strategy refers to the aims of undermining and replacing incumbents in the market. The writer names Xerox photocopiers and Google advertising practices as examples of disruptive innovation strategies.
\item \textsuperscript{356}Evans 2016, p. 3.
\item \textsuperscript{357}The notion of specialized assets was introduced in the US competition policy already in 1995. It was later incorporated in the EU Horizontal Guidelines 2011 (para. 120). The EC Guidelines only refer to patents and know-how as examples of specialized assets, which might not be adequate in the modern data-driven economy.
\item \textsuperscript{358}Graef 2016A, p. 115.
\item \textsuperscript{359}For the role of big data as a source of market power, see for example Schepp 2016.
\item \textsuperscript{360}Graef 2016A, p. 115. See also Körber 2015, p. 3.
\item \textsuperscript{361}O’Donoghue 2013, p. 146. Multi-sided platforms with demand interdependencies often pose challenges for the calculation of market shares. Their market shares on different sides of the platform may not be equal and the calculation may face challenges as many of the services are free or offered at a subsidized price (see Evans 2013, p. 19-22).
\end{itemize}
sided platforms compete not only in the product market for specific services, but also in the market involving more extensive economic use of data.\textsuperscript{362} For this reason, the employment of a more forward-looking approach towards the relevant market would enable analysis extending beyond current use of data in a narrowly-drawn relevant market.\textsuperscript{363}

The delimitation and assessment of potential markets for data to support the traditional relevant market analysis would possibly enable better reflection of the competitive reality in which many multi-sided businesses, such as online platforms, operate. This approach could also enable to evaluate the possible competitive constraints related to the key asset in a specific case to which potential competitors of the incumbent firm need access to be able to challenge and compete in the relevant market in the future.\textsuperscript{364} On the other hand, if the starting point for the definition of relevant markets would be the internally used and generated inputs to other products, critics could argue that the number of market to be analysed might eventually be endless.\textsuperscript{365} Nevertheless, choosing a too narrow approach when assessing data as an essential business asset would ignore the fact that data collection and behavioural monitoring of individuals enable online business operators to develop their services and follow the potential trends in the market.\textsuperscript{366} In the previous years, competition authorities have only examined the effect of data concentration on a firm’s market position only in the advertising context.\textsuperscript{367}

As previously discussed, economic analysis of multi-sided markets may require modification of the traditional methods or even development of completely new approaches to multi-sided businesses.\textsuperscript{368} This might result in improper regulation recommendations and overly marginal role of the digital business models in economic policy analysis.\textsuperscript{369} Although one of the key goals of the GDPR is to strengthen data subjects’ control over their personal data, Engels argues that also the GDPR fails to fully answer to these newly emerged challenges.\textsuperscript{370} Partly for these reasons, the direct effects of the new European data protection legislation on competition, especially the impact of the right to data portability introduced by article 20 GDPR, should be further analysed.\textsuperscript{371} By nature, many platforms have the tendency and ability to rapidly achieve scope and large market valuation using methods that often involve extensive personal data processing. The special characteristics of these digital businesses, especially network effects, congestion, differentiation, economies of scale and

\textsuperscript{362} According to Harbour and Kozlov, defining a separate market for data would better describe the commercial intentions of data processing companies that often expand beyond the initial purposes for which the user data was collected in the first place (Harbour 2010, p. 784).
\textsuperscript{363} Graef 2016A, p. 115.
\textsuperscript{364} Graef 2015A, p. 494-495.
\textsuperscript{365} See Tucker 2014, p. 4-5. The relatively critical writer argues that personal data could not constitute a relevant product market unless sold to customers. Without these transactions, personal information would not satisfy the hypothetical monopolist test, as there would be no product substitution.
\textsuperscript{366} Graef 2016A, p. 115.
\textsuperscript{367} Ibid., paragraphs 78 and 110.
\textsuperscript{368} For example, Alexandrov 2011, p. 15.
\textsuperscript{369} Monopolkommission 2015, p. 122-125 and Engels 2016, p. 2.
\textsuperscript{370} Engels 2016, p. 1-2 and Recital 68 GDPR.
\textsuperscript{371} The right to data portability in the context of EU Competition law is further discussed in chapter 5.
switching costs, might be left out from the privacy considerations when new data protection provisions are designed. They also tend to increase market concentration in the digital platform markets. 372

The following merger case concerning the privacy issues in the acquisition of the freeware and cross-platform service operator WhatsApp, Inc. (WA) by the social networking platform Facebook, Inc. (FB) illustrates the growing importance of personal data in the business strategies of many online platform companies commercially exploiting big data. 373 Secondly, the case embodies how competition authorities seem to be increasingly concerned about the privacy and data protection issues in merger control reviews. Thirdly, this fact might partly indicate a change in the European approach traditionally excluding data protection concerns from the competition law assessment. 374

3.3.3 The second Facebook/WhatsApp merger procedure [2017]

The modified personal data may reflect the business practices of a company controlling data processing activities. 375 As a result, competition authorities seem to be increasingly interested in aspects such as the impact of big data on market power and data collection by smart devices as well as of possible exclusionary conduct of dominant undertakings. 376 In May 2017, the European Commission assessed these concerns in the second Facebook/WhatsApp merger procedure. This merger procedure concerned privacy related matters, not the economic effects of the concentration.

In the first Facebook/WhatsApp merger decision in 2014, the European Commission had approved the acquisition of WhatsApp by Facebook. WhatsApp's annual turnover being under the reporting threshold of the EUMR, the case only came before the EC under art. 4(5) EUMR. 377 In the 2014 decision, the Commission assessed market power in three relevant markets and found that there were no potential horizontal anti-competitive effects in the relevant markets. 378 It also stated that market share analysis was not sufficient indicator of market power in the consumer communications sector. This conclusion was based on the facts that the fast-growing and recent sector was characterised by short innovation cycles and well as frequent market entry. 379 Other reasons for this conclusion included existing alternative

372 Engels 2016, p. 2. See also Geiger 2015.
373 Case COMP/M.8228 Facebook/WhatsApp II [2017].
374 For the traditional approach, see section 2.4 and Case C-238/05 Asnef-Equifax [2006], ECR I-11125, para. 63.
376 Yoo 2012, p. 1154-1158. For the abusive practices related to data, see chapter 5.
377 Case COMP/M.7217 Facebook/WhatsApp I [2014], paragraphs 9-11. The firms' market shares were also greater in the European Economic Area than at worldwide level (para. 39). Interestingly, Ceriello points out that without the 2004 amendments to the EUMR, the FB/ WhatsApp merger would not have been subject to EC’s review but instead to review of several member states separately (Ceriello 2017, p. 495).
378 Ibid., para. 191. For the definition of relevant market for online platforms in the decisional practice of the EC, see chapter 4.
379 Case COMP/M.7217 Facebook/WhatsApp I [2014], para. 99. With this statement, the Commission seems to have admitted the fact that market shares as well as the market definition were constantly evolving (Stakheyeva 2017, p. 267).
services and low switching costs for consumers.\textsuperscript{380} Interestingly, although it had stated that the privacy-related concerns in the case did not fall within the scope of the EU competition rules, it seemed likely that the potential for data collection and online advertising was behind the merger from Facebook’s point of view.\textsuperscript{381}

Two years after the approval, the EC had second thoughts about the Facebook/WhatsApp transaction.\textsuperscript{382} The new procedure focused on privacy and data protection related matters. During the previous proceedings, Facebook had represented that if would not merge the user data between WhatsApp and Facebook, maintaining the relatively strict privacy code of WhatsApp.\textsuperscript{383} However in 2016, Facebook announced that it would in fact use WhatsApp’s personal data to support FB advertising (so-called user matching). Consequently, the Commission requested further clarifications from the parties, in particular on the consistency between the previous statements.\textsuperscript{384} In its decision in 2017, the EC stated that Facebook had ‘at least negligently supplied incorrect or misleading information’ in the previous merger proceedings. According to the EC, Facebook had been ‘well aware’ of the importance of the aforementioned information for the Commission’s assessment. The company was eventually fined €110 million for infringing the article 14 EUMR.\textsuperscript{385}

Interestingly, the Italian antitrust and consumer protection authority AGCM also adopted two decisions in its proceedings against WhatsApp in May 2017. Initiated under the consumer protection mandate of AGCM, both proceedings concerned WhatsApp’s privacy policy and terms of service. While one of these decisions concluded that WhatsApp’s practice of obtaining user consent for the update of its terms was aggressive and unfair, the other one established the unfairness of specific contractual clauses of WhatsApp’s terms of service.\textsuperscript{386}

The privacy-issues reviewed in the proceedings may reflect the growing importance of personal data in M&A strategies of many digital platforms. At the time of the second EC decision in May 2017, the German Federal Cartel Office (Bundeskartellamt) was already investigating Facebook’s usage of WhatsApp’s user data and analytics in Germany. The purpose was to find out whether Facebook abused its dominant position on social networks in the German market.\textsuperscript{387} According to Engels, the degree of market concentration\textsuperscript{388} of social networking platforms was medium in 2016, but with

\textsuperscript{380} Ibid., paragraphs 101-115.
\textsuperscript{381} Ibid., para. 164. See also Case COMP/M.6281 Microsoft/Skype [2011], where the Commission had already pointed to the growth of Facebook as a rapidly growing entrant in the consumer communications market (para. 93).
\textsuperscript{382} Bloomberg Technology 9.9.2016.
\textsuperscript{383} Ibid., para 30. See also EC Press Release 20.12.2016.
\textsuperscript{384} Case COMP/M.8228 Facebook/WhatsApp II [2017], para. 30-31.
\textsuperscript{385} Ibid., paragraphs 100, 107-108 and EC Press Release 18.5.2017. Since the approving merger decision in 2014 was based on a number of different factors beyond the privacy concerns, this decision did not have an impact on the clearance (EC Press Release 20.12.2016).
\textsuperscript{386} Zingales 2017, p. 553-558. The article also clarifies the background and details of the investigations. See also AGCM 12.5.2017.
\textsuperscript{387} Bundeskartellamt Press Release 2.3.2016 and Schweda 2016, p. 420-421.
\textsuperscript{388} For the notion of concentration, see for example case C-248/16 Austria Asphalt [2017], ECLI:EU:C:2017:643, paragraphs 34-35.
potential to increase substantially. Facebook’s behavioural business pattern also is likely to indicate the emerging role of big data as a source of market power and a key business asset in the online platform industry. The Commission’s passivity in the protection of competitors could be a result of balancing the rights and needs of competitors and consumers. Too strong protection might be harmful for consumers and endanger their access to developing technologies.

Regarding the data protection issues and the protection of personal data as a fundamental right in Europe, the extensive collection and use of personal data by Facebook raises questions concerning the portability of this, often sensitive, information. Multi-sided businesses have growing incentives to prevent their rivals’ access to big data sources. Simultaneously they may seek to tighten their data sharing policies and restrain from any portability improvements to protect their data related competitive advantages. In the context of social networks, it is becoming increasingly difficult for individuals to change the social network operator. It could even be argued whether the lack of substitutes and consumer choice are at risk as Facebook has twice as many monthly users as the second largest provider, China’s Tencent. Therefore, consumers might not have adequate alternative, effectively preventing de facto the transfer of data to other platform service providers.

3.4 Preliminary conclusions on chapters 2 and 3

The main purpose of chapters 2 and 3 has been to describe the core notions and rationale behind data protection and competition law. In order to understand their internal logic, the functioning of these systems has to be internalized. For this reason, the first part of this thesis has been somewhat theoretical and the main focus has been on the key rules, definitions and the possible interaction between them.

Against the historical background and development of the European data protection legislation, it is not surprising that many provisions and their implications of the GDPR seem still relatively new and unknown. It seems natural that the rapidly growing importance of big data and data analytics for modern and increasingly digital business models is likely to create risks both in the context of data protection law and competition law. As partly described in chapter 2, many of the early CJEU cases concerning the application of the DPD do not include elements essential to big data. Thus, at this point, it seems to be relatively difficult to approach many of the data protection issues concerning these vast amounts of datasets collected, stored and processed by public and private entities within the meaning of the GDPR. Consequently, some of the thoughts, academic arguments and considerations presented in the thesis may be to some extent speculative by nature.

Concerning this aspect, see for example Song 2017, p. 669-670.
Article 20 GDPR protects data subjects’ right to data portability. See Chapter 5.
OECD: Data-Driven Innovation Report 2014, p. 6 and 42. See also Stucke 2016, p 39-42.
Song 2017, p. 670.
An important conclusion in the chapter 2 is that online environment is likely to create new and increasingly complex circumstances for the application and interpretation of European data protection law. Traditionally, obtaining the data subject’s consent has been one of the key concerns in the European data protection discussion. However, since the introduction of the DPD in 1995, the digital business reality has radically changed. New concepts and rights, such as group privacy\textsuperscript{395}, data subject’s consent obtained in electronic form and right to data portability\textsuperscript{396} are likely to make things more intricate and the risks for potential personal data infringements may also increase.\textsuperscript{397} The commercial exploitation of big data has also developed the online behaviour of many companies. The increasing use of behavioural discrimination in e-commerce is a good example of these practices.\textsuperscript{398}

In the chapter 3, a central aim was to illustrate the importance of market power when assessing possible breaches of competition law, especially in the assessment of abuse of dominance under article 102 TFEU and in merger control activities under the EUMR. As in the case of data protection efforts, competition law enforcement will face challenges in the digital age as well. Many of the traditional concepts and methods used will have to be rewritten and this somewhat confusing legal uncertainty is also partially reflected in chapter 3. Since personal data are becoming an increasingly valuable business asset for many companies, market power may also limit the individual control over personal data, effectively compromising the fundamental principles of the European data protection policy. The second Facebook/WhatsApp merger procedure and the related WhatsApp investigations in Italy seem to support this finding. This aspect is also closely related to the principle of fairness and individual informational self-determination, concepts that that are further discussed in chapter 5 when discussing the data-related abusive acts and practices in the digital marketplace.

In the second part of the thesis (chapters 4 and 5), the principal aim is to apply and develop the key concepts, thoughts and analytical patterns presented in chapters 2 and 3. Chapter 4 seeks to analyse the data protection issues related to data-driven mergers, often concerning multi-sided platforms and big data elements. The definitions of relevant market and the assessment of market power are assessed in selected merger decisions of the European Commission. The chapter 5 further discusses the intersection of data protection and competition law by assessing the competitive concerns related to the right to data portability introduced by article 20 GDPR. Hence, by applying the concepts presented in chapters 2 and 3, the overall purpose is to reflect data protection interests in the context of economic competition within the European Union.

\textsuperscript{395} See section 2.2.1.
\textsuperscript{396} See chapter 5.
\textsuperscript{397} In the context of personal data protection, the French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés, CNIL) has defined the concept of risk as follows: “risk is a hypothetical scenario that describes how risk sources could exploit the vulnerabilities in personal data supporting assets in a context of threats and allow feared events to occur on personal data, thus generating impacts on the privacy of data subjects” (sentence reformulated in article Böröscz 2016, p. 469).
\textsuperscript{398} See for example Ezrachi 2016A.
4.1 On the nature of data-driven mergers

A merger in the narrow sense refers to an activity, where two separate undertakings merge entirely into a new entity. However, in the competition policy context, the concept can be understood as covering a wider range of different corporate transactions. According to the EU Merger Regulation (EUMR), the decisive factor is that it is possible for the merging firm A to exercise decisive influence over the merging firm B. Another possible arrangement, a joint venture, refers to two or more undertakings merging part of their businesses into a new company. In many cases, the acquisition of specific assets can be behind these transactions. However, the general purpose of merging firms is often to increase the market power of the newly born entity and decrease competition in the market.

As explained in chapter 3, online platforms operating in the digital business environment are often considered multi-sided businesses. Through their products and services, they bring consumers and advertisers to a common ground, where interaction, trading and advertising can take place. Whereas users benefit from the quality of the functionalities and services provided through the collected and processed data, advertisers can exploit the detailed profiles of platform users for example by increasing the effectiveness of their marketing efforts and the amount of purchases resulting from their advertisements. In its early merger decision Travelport/Worldspan concerning platform industry, the European Commission already acknowledged the two-sided nature of platform markets in the context of electronic travel distribution services.

Because of the multi-sided nature of these services and the link between two customer groups, it might not be adequate to assess the relevant market for each side of the platform separately. If the company operates on both sides of the platform and adopts its pricing and production decisions accordingly, merely one-sided approach

---

399 In the general business context, a merger refers to the combination or amalgamation of a commercial company, institution, etc. with another entity. It can also refer to the consolidation of two or more companies, etc., into one (Oxford English Dictionary, online version). In this thesis, this term is used to describe all possible phenomena included in the concept.

400 In the European Union, the rules governing the control of mergers are contained in the EU Merger regulation (EUMR).

401 Whish 2015, p. 853. In many cases, even the acquisition of a minority shareholding can be sufficient to constitute a merger.

402 For the concept of control, see article 3(2) EUMR.

403 Whish 2015, p. 854.

404 In the Blokker/Toys ‘R’ Us merger case, the valuable asset was a well-known brand name (Case IV/M.890 Blokker/Toys ‘R’ Us [1997], paragraphs 95-98). Other important merger incentives include for example economies of scale and scope as well as other efficiencies (Whish 2015, p. 857-858).

405 Whish 2015, p. 859.


407 Case COMP/M.4523 Travelport/Worldspan [2007], paragraphs 10-11. However, the Commission only defined one relevant product market in this case (para. 10). See also Filistrucchi 2013, p. 15.
would be likely to lead to erroneous assessments of competitive strength.\textsuperscript{408} Consequently, if the exchange of products or services takes place only at one side of the market, insufficient information may expose the market definition to risk.\textsuperscript{409}

Due to its forward-looking characteristics, the focus of merger control is on the potential harmful effects to competition in the future. For this reason, the approach is also partly theoretical: the competition authority applies a \textit{theory of competitive harm} in order to assess the possible implications for the market and consumers. Nevertheless, as corporate mergers are common in the free market economy, these proceedings should not be based solely on speculation. Therefore, sufficient \textit{evidence} is required.\textsuperscript{410} As many of the traditional economic approaches used in the assessment of the relevant market do not always apply to online platform environment, this task of delimitation has turned out to be relatively challenging for competition authorities.\textsuperscript{411}

It has also even been argued whether the purely \textit{turnover-based thresholds} of the EUMR can be applied to platforms as they have originally been designed for the purposes of traditional sectors of economy.\textsuperscript{412} The target companies may not always have significant turnovers.\textsuperscript{413} However, the monetary turnovers may not always sufficiently reflect the valuable datasets firms may possess.\textsuperscript{414} The fact that the European Commission launched a public consultation in October 2016 in order to, among other things, evaluate the effects of these rules to certain sectors, such as digital and pharmaceutical industries, illustrates the growing importance of this aspects.\textsuperscript{415}

\section*{4.2 Decisional practice of the European Commission}

As the European Commission is rethinking the use of financial thresholds as the only element in merger control procedures, it seems to be important to discuss some of the EC merger cases concerning big data advantages.\textsuperscript{416} A common feature for the following big data merger cases is the specific business strategy to obtain competitive advantages to support the innovative and often ground-breaking commercial activities. This business purpose is achieved by informative means, often by access to personal data. Currently, competition authorities in many jurisdictions have been considering the renewal of the approaches towards mergers involving digital elements and use of big

\begin{itemize}
  \item [408] Graef 2016A, p. 86.
  \item [410] Whish 2015, p. 862-863.
  \item [411] Holtzweber 2017, p. 564. See also Davilla 2017, p. 378.
  \item [412] See for example KKV 2017, p. 21.
  \item [413] For example, in the \textit{Facebook/WhatsApp} merger, WhatsApp only had annual reportable turnover of $20 billion, below the reporting threshold of the EUMR (Case COMP/M.7217 Facebook/WhatsApp I [2014]). See also Ceriello 2017, p. 495.
  \item [414] Stakheeva 2017, p. 181.
  \item [415] Interestingly, Microsoft stated in its response to this public consultation, that there was no general need for data-related changes in the EUMR thresholds in order to cover the big data related transactions. The firm’s response might indicate that it wanted to underrate the competitive value and importance of big data for digital businesses (EC Consultation 2017 Microsoft Response, p. 2-6).
  \item [416] Examples of big data mergers not further analysed in this chapter include for example the following: Case COMP/M.4853 TomTom/Tele Atlas [2008]; Case COMP/M.4726 Thomson Corporation/Reuters Group [2008]; Case COMP/M.6314 Everything Everywhere [2012] and Case COMP/M.7337 IMS Health [2014].
\end{itemize}
data. In addition, the intersection of data protection and privacy issues in the big data mergers may require further research and analysis. Although traditionally left outside the scope of competition law Stakheyeva and Toksoy argue that these two regimes are inseparable in merger cases involving big data elements.\footnote{Stakheyeva 2017, p. 265-266.}

\subsection*{4.2.1 Google/DoubleClick [2008]}

One of the early examples of mergers including big data considerations was the acquisition of ad service provider DoubleClick by the active search engine platform, online intermediary and advertising space seller Google, Inc.\footnote{Case COMP/M-4731 Google/DoubleClick [2008].} This transaction was eventually cleared by both the US Federal Trade Commission and the European Commission, finding no anti-competitive effects on any of the relevant markets defined.\footnote{Kadar 2017, p. 180. For the US case, see Abramson 2008, p. 659-661.} While DoubleClick was a leading service provider in the market, its core business model was only an ancillary service in Google’s service repertoire.\footnote{Ibid., paragraphs 192-202.} Google’s main purpose was to obtain exploit DoubleClick’s valuable data in its personalized and targeted advertisement practices.\footnote{Stakheyeva 2017, p. 183.}

In the assessment of the relevant market, the Commission identified the multi-sided nature of these online advertising intermediation services.\footnote{For example Alexiadis 2017, p. 100-101.} However, in its evaluation, the Commission did not assess the markets for advertisers and publishers separately, focusing instead on the reality of an intermediation market.\footnote{Case COMP/M-4731 Google/DoubleClick [2008], paragraphs 72-73.} This market was considered separate from the market for direct sales. Thus, the Commission defined a single market for online intermediation. Although these conclusions did not provide an explicit definition of a single relevant market, the Commission’s definition seemed to be correct in the light of the transactional nature of the platforms in question. Interestingly, had the EC recognized or discussed the potential for one or more relevant markets for users of Google’s websites, it could possibly have observed the data-related potential of DoubleClick acquisition for Google. After the transaction, the company could acquire personal information on online users and use these datasets to improve its targeted advertising practices on its websites.\footnote{Graef 2016A, p. 336.}

In its assessment of competition concerns, the Commission stated that the main source of the competitive constraints for DoubleClick were other ad services rather than Google. The Commission also assessed different foreclosure strategies in relation to the leveraging of DoubleClick’s leading market position and the possible synergies concerning the combination of the firms’ databases.\footnote{Ibid., p. 74-97.} Some of the third-party complainants had stated that Google was able to attract DoubleClick’s customers to use its own intermediary platform services and the acquisition of DoubleClick’s data
resources would reinforce the ability. Especially Google’s capability of using these data to develop more accurate targeted advertising could be considered an essential strategy. The increased use of targeting would in turn attract more advertisers and publishers to use Google’s services, effectively constituting a significant competitive advantage for Google.\footnote{Kadar 2017, p. 480.}

However, the European Commission dismissed these concerns after only a few respondents had confirmed Google’s advantages concerning the access to DoubleClick’s datasets. In addition, third-party complainants had argued that the \textit{post-merger combination of data} would make Google’s position impossible to challenge. The Commission dismissed these arguments as well. First, DoubleClick’s relevant contracts with publishers prevented the use of customer data in the service development by others than the actual contractual parties. The merged entity, additionally, would not have been able to easily impose contractual changes as it was not in the interest of the other parties. Second, DoubleClick’s data was not considered to be an essential input for effective online advertising. These datasets could be substituted by data collected by third-party entities, other service providers or developed in-house.\footnote{Case COMP/M-4731 \textit{Google/DoubleClick} [2008], paragraphs 359-366.}

In essence, the decision of the EC may have reflected the interpretation of the CJEU’s \textit{Asnef-Equifax} judgement when the Commission left aside the actual data protection interests. Instead, it focused on the competition concerns resulting from the combination of different datasets.\footnote{Graef 2016A, p. 326.} Thus, while it did not assess the effect of the Google/DoubleClick merger on privacy and personal data protection as such, it did analyse several related issues to the extent relevant for the competition concerns at hand. In the Google/DoubleClick case this data-related concern was the potential impact on the market of the different combinations of datasets.\footnote{Ibid., p. 335-336.}

\subsection*{4.2.2 Microsoft/Yahoo Search Business [2010]}

The acquisition of \textit{Yahoo Search Business} (YSB) by technology company \textit{Microsoft, Corp.} in 2010 was an early example of a merger between two search engine providers in a complex and dynamic two-sided market.\footnote{Case COMP/M.5727 – \textit{Microsoft/Yahoo} [2010]. See also Vecchi 2010.} The merger included both the internet general search functionalities and the corresponding advertising platform (\textit{Panama}) of YSB. Microsoft was also involved in internet general search and online advertising business with its equivalent service platforms (\textit{Bing} and \textit{adCenter}). Eventually, the European Commission cleared the merger unconditionally, stating that it did not have anti-competitive effect on competition.\footnote{Case COMP/M.5727 – \textit{Microsoft/Yahoo} [2010], paragraphs 250-256. However, the merger did raise questions concerning privacy related issues (see for example Lande 2008).}

The case was significant, as it was the first time when the Commission applied competition law to internet search services. It distinguished \textit{horizontal and general}}
search business from vertical internet search. However, it did not take a position for or against a separate relevant market. Consequently, the Commission assessed the legality of the merger only with regard to online advertising market. Nevertheless, the EC took into account the possible link between the user side and advertisers when it examined the potential anti-competitive effects of the merger on innovation, relevance and variety of internet search to users. According to Evans, the Commission seem to have considered both market sides forming together a certain type of business ecosystem, in which none of the sides can be assessed in isolation. In the competitive assessment, the Commission recognized the increase in concentration, as the number of market operators decreased from three to two. In addition, the search markets of Microsoft and YSB were characterized by high market barriers to entry. Although Microsoft had pursued the goal of becoming a credible alternative to Google, the online advertising market leader, it would not have been able to reach this target without the transaction.

However, the Commission’s data-related issues in the Microsoft/YSB merger concerned especially the following three elements: barriers to entry, possible beneficial effects of the merger and the relevant counterfactual. Both companies, competing with Google, had difficulties to achieve the “critical mass” scale. With this term the Commission referred to the sufficient internet traffic volume to make them attractive in the eyes of advertisers and alternatives for Google. The Commission also stated that it seemed clear that new market operators needed significantly costly and large databases in order to be able to enter the market. Finally, the EC considered the pro-competitive effects of the merger. The increased scale of the new entity enabled the competition against Google more effectively. With increased query volumes, Microsoft was more likely to be able to personalize and improve its search services. This in turn was likely to lead to better user experience and through the generation of ad inventory, more advertisers were also expected to use the platform. In other words, the essential conclusion in the case was that the scale of big data collection was likely to lead more relevant search results.

432 Ibid., para. 31.
434 Case COMP/M.5727 – Microsoft/Yahoo [2010], paragraphs 85-87.
435 Ibid., paragraphs 202-226.
436 Evans 2011, p. 21-22.
437 Case COMP/M.5727 – Microsoft/Yahoo [2010], paragraphs 12-26.
438 Ibid., para. 111. The according to the Commission, these entry barriers included hardware, human capital, cost of web indexing, development and update costs of algorithms as well as IP patents.
439 Ibid., para. 148. In addition, the Commission considered Yahoo’s market performance stating that its performance was declining (paragraphs 137-147).
440 Kadar 2017, p. 480.
441 Case COMP/M.5727 – Microsoft/Yahoo [2010], para. 153.
442 Ibid., para. 111.
443 Case COMP/M.5727 – Microsoft/Yahoo [2010], paragraphs 250-256. Microsoft argued that with larger scale of data collection, it could run algorithm improvement tests. This is also relevant in the context of machine learning.
444 Graef 2016A, p. 47. Interestingly, in its statements, Google tried to depreciate the importance of the economies of scale in data collection, referring to the declining value of incremental data when the data amounts increase (para. 174).
4.2.3 Microsoft/Skype [2011]

In the Microsoft/Skype merger case the European Commission assessed the acquisition of a Luxembourg-based telecommunications software company, Skype, by Microsoft.445 Microsoft, being one of the largest companies in the US and also a significant market force worldwide, sought to obtain Skype’s customer base of over 650 million users and to benefit from the acquisition of a well-established internet telecommunications platform. The European Commission had standing to review the case because the revenues of the parties involved satisfied the EU dimension requirement.446 After its assessment, the EC decided not to oppose the transaction.447

In its assessment of the relevant market, the Commission stated that the relevant product market in the case consisted of both enterprise and consumer communications markets. However, it agreed with the merging parties determining that these two markets were distinct for purposes of competition analysis due to the different functionalities of the services and the purposes of businesses and consumers in using online telephone platforms. Microsoft and Google were the only companies providing both consumer and business services. Skype’s customer base was strongly consumer-oriented. In addition, businesses were willing to pay for Skype’s services whereas these services were free to consumers. Therefore, the EC concluded that the consumer communications and enterprise communications services formed two distinct product markets and were assessed separately.448

The EC stated that the high market share resulting from the concentration could not be directly translated into market power or assumed to harm competition. It also stated that market share in consumer communications sector could change within a short period of time.449 Firstly, the market for Internet-based consumer communications was characterized by rapid innovation cycles. This feature tends to improve the competitive impact of both smaller and larger market shares over the long term.450 Secondly, Skype was already pre-installed in a major portion of personal computers using Microsoft’s operating system but only “few” users actually were registered users of the platform.451 It was also relatively easy for consumers to switch services as individuals were often communicating with only small group of people making the coordination of the move simple.452 Thirdly, according to the Commission, the major growth in internet based consumer communications was taking place in the market for smartphones and tablets, where Microsoft had a weak market position with its Windows Phone.453 Although it recognized the possibility of certain weak barriers of entry, it also acknowledged the fact that a new market entrant could rapidly and significantly change the market power.

445 Case COMP/M.6281 Microsoft/Skype [2011].
446 Ibid., para. 5 and article 1 EUMR.
447 Ibid., para. 223.
448 Ibid., paragraphs 10-17.
449 Ibid., para 78.
450 Ibid., para. 168.
451 Ibid., para. 161-162.
452 Ibid., para. 130.
453 Case COMP/M.6281 Microsoft/Skype [2011], paragraphs 163-165.
of the merged entity.\textsuperscript{454} As an interesting detail from the case, the EC also mentioned the growth of Facebook as a new market entrant.\textsuperscript{455}

The Commission’s decision to clear the merger was followed by an appeal in the General Court.\textsuperscript{456} Two firms, Cisco Systems and Italian Messagenet sought the annulment of the EC decision. In its judgement in 2013, the General Court confirmed almost entirely the decision and rationale of the Commission.\textsuperscript{457} The Court maintained that the Microsoft/Skype merger had to be distinguished from earlier cases concerning Microsoft as there were no economic or technical constraints preventing users from using other services.\textsuperscript{458} It continued stating that the Commission had assessed even the most narrow market definitions and analysed different user platforms although it did not separate the consumer and business user side of the market.\textsuperscript{459}

In August 2013, Microsoft announced that it would seek to bundle Skype with its newly developed operating system.\textsuperscript{460} According to Ceriello, the fact that this business decision has not raised competition concerns might reflect the rapid evolution of the market for operation systems. Microsoft has also been losing in the market for Android systems as cell phone technology is gaining ground as a preferred online search method.\textsuperscript{461}

\subsection*{4.2.5 Facebook/WhatsApp I [2014]}

In early 2014, Facebook, Inc. (FB), the largest social media platform in the world, announced the intention to acquire WhatsApp, Inc. (WA) in a transaction worth approximately $19 billion.\textsuperscript{462} According to Ceriello, the Facebook/WhatsApp merger was ground-breaking due to the business model and the size of the transaction.\textsuperscript{463} WA’s annual turnover being under the reporting threshold of the EUMR, the case only came before the EC under article 4(5) EUMR.\textsuperscript{464} WhatsApp was relatively new provider of web-based communications services. At the time of the merger review, WhatsApp had more than 450 million active users (300 million in Europe) and Facebook 1,3 billion worldwide. The company was also expanding rapidly in the market.\textsuperscript{465}

The European Commission identified three relevant markets in its analysis: consumer communications services via mobile phone, social networking services and

\begin{footnotes}
\textsuperscript{454} Ibid., para. 87.
\textsuperscript{455} Ibid., para. 93.
\textsuperscript{456} Case T-79/12 Cisco Systems [2013], ECLI:EU:T:2013:635. See also Graef 2014, p. 1269-1279.
\textsuperscript{457} GC Press Release 156/2013.
\textsuperscript{458} Case T-79/12 Cisco Systems [2013], ECLI:EU:T:2013:635, para 79.
\textsuperscript{459} Ibid., para. 66.
\textsuperscript{460} Geek 16.8.2013.
\textsuperscript{461} Ceriello 2017, p. 501.
\textsuperscript{462} Case COMP/M.7217 – Facebook/WhatsApp [2014]. For more specific details concerning the competitive assessment in the first Facebook/WhatsApp merger case, see section 3.3.2.1.
\textsuperscript{463} Ceriello 2017, p. 494. See also the Google/DoubleClick merger case in section 4.2.1 (Case COMP/M.4731 [2008]) where both companies held large amount of customer-provided data on browsing behaviour and consumer online search (paragraphs 179-181).
\textsuperscript{464} Case COMP/M.7217 – Facebook/WhatsApp [2014], paragraphs 9-11.
\end{footnotes}
The geographic market of the companies was at least the entire EU if not worldwide. As in Google/DoubleClick and Microsoft/YSB cases, the Commission was not forced to decide whether separate relevant markets existed for search and non-search advertising. The reason for this was that the EC did not find serious doubts concerning the compatibility with the internal market in any of the market segments in question.

The EC analysed the potential data concentration effects of the merger in the online advertising market but found no reason that would raise competitive concerns. The Commission also stated that the traditional market share analysis was not indicative of horizontal anti-competitive effects. The reasons for this conclusion included ease of entry into the market, low switching costs for customers and other alternative services available. In addition, there were a significant difference in the user experiences of the merging firms’ applications (Facebook Messenger and WhatsApp). The Commission found that the two companies were not close competitors in the consumer communications market. It noted that the technical difficulties related to integration of the user networks of the merging companies.

The Commission also discussed data portability issues in its decision. Several telecom companies operating in the consumer communications market had indicated that the switching costs for consumers would include loss of all data and interaction history when changing consumer communications applications. However, the EC had not found any evidence pointing out that data portability issues were likely to constitute a barrier of entry in the case. It was highly unlikely that this right protected by article 20 GDPR would be at risk since WhatsApp’s contact list could be ported effectively giving a competing application access to these data. It was also possible to consumers to keep the messaging history in their smartphones.

In the 2014 decision, the European Commission cleared the transaction finding that there were no anti-competitive effects in the relevant markets. Interestingly, although it had stated that the privacy related concerns in the case did not fall within the scope of the EU competition rules, it seemed likely that the potential for data collection and online advertising was behind the merger from Facebook’s point of view. Thus, the future business models of online advertising and data collection provided an important basis for the transaction. In addition, the concept of revenue expanded beyond the traditional merger analysis in this case where all involved services

---

466 Case COMP/M.7217 – Facebook/WhatsApp [2014], paragraphs 3-14.
467 Ibid., para. 44.
468 Graef 2016A, p. 102.
471 Case COMP/M.7217 – Facebook/WhatsApp [2014], p. 18.
472 Ibid., paragraphs 101-107 and 123.
473 Ibid., para. 113.
474 Ibid., para. 191. A few of the responding firms had indicated that the lack of data portability and interoperability between different platforms would constitute an entry barrier if merger was to be cleared (para. 122). See also EC Press Release 3.10.2014. For a competition law approach to software interoperability, see for example Graef 2013A.
475 Ibid., para. 164.
were free to consumers.\cite{Ceriello2017} The fact that the transaction did not have the EU dimension raises questions whether it is necessary to introduce an alternative “value of transaction” threshold for the purposes of merger control.\cite{Stakheyeva2017}

### 4.2.4 Publicis/Omnicom [2014]

In the transaction between Omnicom, a US-based global marketing, advertising and corporate communications company and Publicis, a French international advertising service provider the intention of the merging parties was to create the world’s largest advertising company at the time. Both firms were active in the advertising, marketing and communications services sectors.\cite{Case COMP/M-7023 Publicis/Omnicom [2014], para. 9} The commission eventually cleared the merger, before the created $35 billion entity eventually collapsed.\cite{See Fortune 9.5.2014}

In the case, the EC assessed the market for media buying services and that of marketing and communication services.\cite{Ibid., paragraphs 7-20.} The horizontal overlap between the companies occurred predominantly on the markets for media buying services and marketing communications services.\cite{Kadar2017} The Commission also considered the possibility of non-coordinated effects\cite{Also known as unilateral effects, the notion refers to effects resulting in the merged firm’s profitable price increases due to the loss of competition between the merged parties (see for example Whish 2015, p. 985).} on the market for data analytics services, where both firms were only marginally active through subsidiary companies. However, the combined market share of Publicis and Omnicom in this market was below 15 per cent, the EUMR threshold for the determination of an affected market. Additionally, the EC discussed the potential decrease in access to big data should the merged entity develop its own analytics platform and refuse to give its competitors access. Importantly, it stated that big data analytics was gradually becoming more relevant especially for online business models, such as digital forms of advertising. Within this particular area, there could be identified a large number of big data analytics suppliers. Therefore, the Commission did not find any serious risks arising from the transaction in relation to big data.\cite{Case COMP/M-7023 Publicis/Omnicom [2014], para. 629630.}

### 4.2.6 Sanofi/Google [2016]

The Sanofi/Google case concerned the joint venture between Google and a global pharmaceutical group Sanofi, active in R&D as well as in marketing and manufacturing of healthcare products.\cite{Case COMP/M.7813 Sanofi/Google [2016].} The intention of the parties was to combine Google’s expertise in miniaturised electronics, consumer software development and analytics with Sanofi’s experience in the treatment of diabetes patients. The new entity created

---

\begin{itemize}
  \item \footnotesize{\cite{Ceriello2017} Ceriello 2017, p. 496-497.}
  \item \footnotesize{\cite{Stakheyeva2017} Stakheyeva 2017, p. 266. See section 4.3.1 of the thesis.}
  \item \footnotesize{\cite{Case COMP/M-7023 Publicis/Omnicom [2014], para. 9} Case COMP/M-7023 Publicis/Omnicom [2014], para. 9.}
  \item \footnotesize{\cite{See Fortune 9.5.2014} See Fortune 9.5.2014.}
  \item \footnotesize{\cite{Ibid., paragraphs 7-20.} Ibid., paragraphs 7-20.}
  \item \footnotesize{\cite{Kadar2017} Kadar 2017, p. 481.}
  \item \footnotesize{\cite{Also known as unilateral effects, the notion refers to effects resulting in the merged firm’s profitable price increases due to the loss of competition between the merged parties (see for example Whish 2015, p. 985).} Also known as unilateral effects, the notion refers to effects resulting in the merged firm’s profitable price increases due to the loss of competition between the merged parties (see for example Whish 2015, p. 985).}
  \item \footnotesize{\cite{Case COMP/M-7023 Publicis/Omnicom [2014], para. 629630.} Case COMP/M-7023 Publicis/Omnicom [2014], para. 629630.}
  \item \footnotesize{\cite{Case COMP/M.7813 Sanofi/Google [2016].} Case COMP/M.7813 Sanofi/Google [2016].}
\end{itemize}
through the joint venture (JV) was to provide services concerning the treatment and management of diabetes using an integrated digital *e-medicine platform* developed by Google. These business activities would involve data collection, data processing and big data analytics. As part of the provided services, the results of JV’s big data analytics were intended to be made available to healthcare professionals and patients. Following a Phase I investigation of the European Commission, the transaction was cleared unconditionally.

In the assessment, the Commission considered the possible exclusionary effects on third-party healthcare dataset owners in the case Google would refuse to offer its data analytics tools them after the joint venture was established. The EC stated that there were a large number of alternative providers of healthcare data analytics tools in the market. This specific market was also growing rapidly, indicating a fast market entry into the market by new entrants. As a supporting example, the Commission referred to the existing pharmaceutical companies developing *in-house data analytics tools* for captive consumption purposes. The Commission also addressed concerns about Google *locking-in* patients with diabetes to the JV’s management and treatment services, mainly by preventing or limiting the data portability toward competing services. Because the competitors could potentially establish themselves in the market even before the JV, the Commission did not find sufficient evidence for these claims and it also stated that it was questionable whether the JV could be capable of acquiring substantial market power to fore close its rivals. It was interesting that the article 20 GDPR and the right to data portability was discussed in this case, indicating its growing importance in the platform economy.

In addition, one competitor had raised concerns related to the possible risks to data security and patient privacy, stemming from the business strategy regarding access to data. However, the EC dismissed these claims by stating that the DPD, national legislation as well as the new GDPR required the explicit consent of the patient for the use his data. The use of these data was likely to be heavily regulated due to the sensitive information such as insulin levels, individual’s blood glucose levels and haemoglobin AIC levels. Thus, the substantial degree of data protection offered was, according to the Commission, sufficient to dismiss these concerns.

---

485 Ibid., paragraphs 1-13 and 16.
486 Ibid., para. 86.
487 Ibid., paragraphs 72-77.
488 In economics, the term *lock-in* refers to a period during which a person or company is bound by the terms of a contract or agreement. It can also refer to an arrangement or contract according to which a person or company is obliged to deal only with a specific company (Oxford English Dictionary, online version).
489 Kadar 2017, p. 483-484.
490 Case COMP/M.7813 Sanofi/Google [2016], paragraphs 67-69.
491 Ibid., para 70-71.
4.2.7 Microsoft/LinkedIn [2016]

The $26 billion transaction between Microsoft and LinkedIn, a professional social networking platform was primarily a conglomerate.\(^{492}\) Microsoft’s rationale behind the transaction was to integrate LinkedIn’s network within its own product range. This strategic move was also intended to create significant synergies for the giant of the TMT sector.\(^{493}\) After the merger, Microsoft could add marketing and recruiting services as well as sales to its key business products for next-generation computing.\(^ {494}\) The acquisition of LinkedIn by Microsoft was eventually approved by the Commission with several commitments concerning social networking platforms.\(^ {495}\) These commitments were not directly linked to big data aspects of the merger. Instead, they were aimed at addressing the doubts related to the pre-installation of LinkedIn on personal computers with Microsoft’s operating system and the integration of certain LinkedIn functionalities.\(^ {496}\)

In the assessment of the relevant market, the EC maintained the previously formulated definitions in the competitive assessment. As in the Facebook/WhatsApp I decision, the relevant product market was found to consist of three sectors: professional social network services, customer relationship management (CRM) software solutions and online advertising services.\(^ {497}\) In the definition of geographic markets, the EC chose a more conservative description when it determined it as EEA-wide although admitting that the scope could be global due to the nature of the Internet.\(^ {498}\)

The main competitive concern in the Microsoft/LinkedIn merger was the potential anti-competitive effects to the market of professional social network services in the EEA. The assessment of horizontal effects was limited to the online advertising market, where the EC evaluated the possible impacts stemming from the post-merger combination of datasets. This information would include personal data, contact information and customer search behaviour.\(^ {499}\) The Commission started the assessment by acknowledging the fact that any data combination can only be implemented in the scope compatible with the relevant national data protection legislation.\(^ {500}\) It also recognized the possible limiting effect of the GDPR on the ability of Microsoft to have access and to process its users’ personal data in the future.\(^ {501}\) By

\(^{492}\) Case COMP/M-8124 Microsoft/LinkedIn [2016]. For the conglomerate nature of a merger, see for example Whish 2015, p. 854-855.
\(^{493}\) Business Insider 8.12.2016. See also Kadar 2017, p. 484.
\(^{494}\) Stakheyeva 2017, p. 266.
\(^{495}\) Case COMP/M-8124 Microsoft/LinkedIn [2016], p. 99 and Annex 1.
\(^{496}\) See Annex 1 of the document: Case COMP/M-8124 Microsoft/LinkedIn [2016].
\(^{497}\) Case COMP/M-8124 Microsoft/LinkedIn [2016], p. 2-32. See also Stakheyeva 2017, p. 266.
\(^{498}\) Ibid., para. 120.
\(^{499}\) Ibid., para 176-177.
\(^{500}\) Both companies in the case were subject to Irish data protection laws as the applicable national data protection legislation was determined by the location where an undertaking has its registered seat and/or where it has the data processing subsidiaries (article 4 DPD).
\(^{501}\) According to the EC, the rules under the GDPR were aimed at empowering individuals with more control over their personal data as well as to strengthen the already existing rights (Case COMP/M-8124 Microsoft/LinkedIn [2016], para. 178).
testing two possible theories of competitive harm, the EC studied two potential impacts of the merging parties’ databases on the market. Firstly, the Commission considered the possible barriers of entry for new entrants created by the increased user database of LinkedIn and the potential increase in the merged firm’s market power. Secondly, it assessed the possible elimination of pre-existing competition between the merging entities, even in the case there would be no post-transaction combination of data. However, the EC dismissed these concerns stating that LinkedIn did not appear to have a significant degree of market power in the upstream market in order to harm the market.

Before dismissing the competitive concerns related to the potential foreclosure of competing software providers, the EC also considered Microsoft’s ability to further increase its dominant position by restricting vertical access to LinkedIn’s databases, effectively hindering innovation in the field of Machine Learning (ML) by competing productivity software solutions. Nevertheless, the Commission found that the transaction was unlikely to enable Microsoft to foreclose the market since LinkedIn’s services did not seem to be “must have” solution or a prerequisite for the competition in this specific market. The combined market share of the merging parties was also relatively small in the market for online advertising, effectively supporting this conclusion.

The big data related discussion in the case was more prominent when the Commission assessed the potential of LinkedIn’s database to become an important input for the provision of ML related CRM software solutions. It also took into account Microsoft’s ability to hinder innovation by restricting its competitors’ access to this input. It remained unclear whether LinkedIn’s pre-merger third-party policy would be sustained as the company had not licensed its full data to third parties prior to the merger. However, the Commission recognized the pro-competitive effects in case Microsoft decided to use LinkedIn’s full data potential to promote innovation by improving its own CRM product.

### 4.3 Emerging data protection and privacy issues in merger control

Several conclusions can be drawn from the merger cases analysed above. Despite the relatively debated role of data protection considerations in the competition law assessment, it seems clear that mergers involving economic use of big data are also likely to include essential privacy and data protection elements that need to be

---

502 For the notion and its dimensions, see for example Whish 2015, p. 862-864.
503 Case COMP/M-8124 Microsoft/LinkedIn [2016], paragraphs 179-180.
504 Case COMP/M-8124 Microsoft/LinkedIn [2016], para. 254. However, it can be argued whether the value of professional information was sufficiently taken into account in the assessment considering the 400 million professionals using LinkedIn and their network of connections (Stakheeva 2017, p. 266).
505 Ibid., paragraphs 234-245.
506 Ibid., paragraphs 265-272.
507 EC non-horizontal merger Guidelines 2008, paragraphs 31. 34.
508 Case COMP/M-8124 Microsoft/LinkedIn [2016], para. 30.
509 Ibid., paragraphs 254-255.
addressed. For example in Facebook/WhatsApp I and Sanofi/Google cases, the new data subject’s right to data portability was discussed, even though no infringements were eventually found. In particular, if the intention behind a specific activity breaching data protection legislation was to gain a competitive advantage over the rivals, this should be the case. In addition, a lower level of privacy resulting from a big data merger involving the removal of a competitor with higher privacy levels or the combination of different datasets might in certain cases decrease the product variety or quality effectively reducing consumer welfare.

Since there is no obligation for the merging parties to notify and obtain the data protection authority’s approval for the merger, the customer privacy and data protection impact assessment of the transaction can only be done within the scope of the merger control procedure by the responsible competition authorities. This means that the administrative burden of the competitive authorities would potentially grow as only they are authorized to make the merger clearance decision conditional on compliance, including with the relevant data protection rules. However, as the case law presented in this chapter has shown, the European Commission has been relatively reluctant to touch upon these issues in recent years.

Despite the key role of financial thresholds as indicators of the importance of a specific merger, the reality may be more complex when the transaction involves significant data-related assets. Partly for this reason, the aforementioned examples of data-driven mergers seek to illustrate the increasing complexity of these transactions in the digital economy. In reality, the value of information and other resources, such as the market presence of a company, innovation and know-how may define the actual value of the digital merger. The introduction of the new size-of-transaction test in German merger control in accordance with the 9th amendment of the German Competition Act and the extended authority of the Federal Cartel Office of Germany also seem to indicate the new emerging challenges. In addition, this development highlights the growing interplay between different EU law regimes, such as competition law and data protection regulation.

It seems to be difficult to actually measure the possible deterioration in privacy conditions of digital services. Especially, it might be difficult to conclude ex ante the worsened data protection conditions without having observed the actual ex post consequences. Schepp and Wambach present that no test equivalent to the SSNIP has been found to sufficiently capture the decrease in quality of a product. Consequently, the case appears to be even more difficult in the context of user privacy. Even if sufficiently effective methods existed, it can always be argued

510 Stakheyeva 2017, p. 270.
511 Schepp 2016, p. 123.
512 Stakheyeva 2017, p. 270.
513 Ibid., p. 268. For further details concerning the renewal of German Competition Act, see section 5.3.2.
514 Costa-Cabral 2017, p. 37. During the recent years, DG Comp’s practice has reflected the doctrine that competition law should seek to achieve benefits for consumers. However, it may be challenging to include data protection considerations in the European Commission’s ‘consumer welfare’ model (Kuner 2014, p. 247-248).
whether it is the task of competition authorities to intervene in this assessment. Nonetheless, despite the possible critique, it could be argued whether more resources should be used in order to strengthen the cooperation between data protection and competition authorities within the EU. This improvement might to some extent prolong the merger review processes, but it may be justifiable as a consumer protection mechanism. Since big data mergers obviously cover two distinctive regimes, competition issues and data protection, competition authorities could take different commitments from the merging parties in order to control the use of personal data in post-merger conditions. This would also allow consumers to have a clearer picture and control over the online information disclosure. These practices would also demonstrate awareness of data protection concerns and good intentions of the relevant stakeholders.

Maybe the most significant example of the European Commission’s reluctance to deal with data protection and privacy in its merger review practices was the Facebook/WhatsApp I decision in 2014. The consequences of this ignorance were seen three years later when the EC had to face the rationale behind Facebook’s business strategy concerning the transaction. The merger was originally cleared despite the fact that future changes in WhatsApp’s privacy policy could be expected. Stakheyeva and Toksoy argue that in the terms of privacy and security, after the terms of privacy of WhatsApp were changed as a result of the merger with Facebook, the enabled transfer of personal data has even led to the deterioration in the quality of the WA’s services.

However, the Microsoft/LinkedIn case could be seen as a positive change in the debate surrounding the interplay between data protection, privacy and competition law. After the transaction was cleared, the EC stated that although not directly falling within the scope of EU competition law, privacy related concerns could be taken into account in the competition assessment. This approach should be limited to the extent that consumers see privacy issues as a significant indicator of quality, and the merging companies compete with each other on this resource. This statement of the European Commission after the Microsoft/LinkedIn merger seem to indicate that it had considered data privacy as an important parameter of competition between social networking platforms. In addition, with this approach the EC appears to have acknowledged the possible negative impacts of the merger on the relevant market.

---

516 See Tucker 2015.
517 Integrating data protection interests in EU competition policy might increase the democratic legitimacy of competition law as the role of non-efficiency interests would become more significant. However, at the same time, too much focus on non-efficiency issues could create more legal uncertainty and make the enforcement activities more complicated (Graef 2016A, p. 326).
519 Ibid., p. 270.
520 Ibid., p. 270. See also Marini-Balestra 2017, p. 5-6.
522 Kadar 2017, p. 270.
5 THE RIGHT TO DATA PORTABILITY IN THE CONTEXT OF EU COMPETITION LAW

5.1 The right to data portability under article 20 GDPR

5.1.1 Scope of application, exercise of the right and rationale

As a new right of data subject introduced by the GDPR, the essential aim of the right to data portability (art. 20 GDPR) is to strengthen and increase data subjects’ control over their personal data. The right covers processing carried out by automated means, in other words by allowing the data subject to transmit his or her personal data from a controller to another.\(^{523}\) The provision can be seen as an extension to the individual’s right to access provided under article 15 GDPR.\(^{524}\) Zanfir suggests that the foundations of this right can be found in the free development of human personality. As the rapid development of the Internet allows individuals to technically live online, the vast amounts of personal data collected, stored and processed in the digital world could even be understood as a continuation of one’s personality. This interpretation would lead to creation of a digital personality of the individual, protected by data protection rules. Considering these arguments, it may seem reasonable to regard data processor’s efforts to block data portability as a violation of fundamental rights.\(^{525}\) According to article 20(1) GDPR:

1. “The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) 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); and

   (b) the processing is carried out by automated means.”

Being a fully original piece of the new European data protection framework, no references to the right to data portability can be found in the previous DPD.\(^{526}\) The improved economic flexibility and the consumer empowerment are likely to facilitate data subject’s ability to copy, move or transmit his or her personal data from one IT environment to another.\(^{527}\) The data subject has the right to request the transmission of

\(^{523}\) Voigt 2017, p. 169. In the context of social networking platforms, the exercise of this right would include for example consumers’ ability to change social network service provider.

\(^{524}\) Bapat 2013, p. 3.

\(^{525}\) Zanfir 2012, p. 151. The right can also be viewed as an addition to the so-called micro rights (such as the right of access to personal data) introduced already in DPD (Lynskey 2017, p. 803). Also Malgieri 2016.

\(^{526}\) De Hert 2017A, p. 2. Interestingly, the Universal Service Directive (2002/22/EC) includes a reference to number portability (article 30 and recitals 40-42). This term can be understood as the practical and theoretical precursor of the later data portability right. See also Graef 2013B, p. 502-514.

\(^{527}\) For strategic reasons, the scope of application of art. 20 GDPR does not cover data generated by the controller as part of personal data processing activities, for example by recommendation or personalization process, user profiling or categorization. However, any merely observed data falls within
its personal data under article 20 GDPR as soon as this information falls within the scope of application.\textsuperscript{528} If the request of data transmission concerns a \textit{large quantity} of personal data, the processor shall have the right to ask the data subject to \textit{specify} the request before taking any actions.\textsuperscript{529} In addition, the transmission shall take place \textit{directly from one controller to another} (art. 20(2) GDPR). Data subjects are always free to transmit their personal data \textit{themselves} as well, after receiving these datasets in a format complying with the regulation (art. 20(1) GDPR).\textsuperscript{530}

Although originally targeted to \textit{social network operators}, data portability is relevant for a variety of other personal data controllers as well.\textsuperscript{531} Nevertheless, it is likely that compliance with article 20 GDPR will require considerable efforts from the controllers as the provision is in many ways consumer-centric by nature.\textsuperscript{532} This emphasis may leave the controllers’ interests more in the background. In other words, guaranteeing the free disposal of personal data to individuals might in some cases endanger the practices and \textit{business secrets} of the controllers.\textsuperscript{533} The processed personal data may often be further processed, for example by classifying or altering the information according to certain criteria. After these modifications, the data might reflect the central processing activities or essential business practices of the controller.\textsuperscript{534} In addition, it is not completely clear what the wording ‘\textit{structured, commonly used and machine-readable}’ means in practice. Although it is explicitly stated in the recital 68 of the GDPR that the right to data portability should not create an obligation for the controllers to maintain or adopt \textit{technically compatible} processing systems, it remains uncertain if the two communicating systems do not embed a communicating transmit module.\textsuperscript{535}

It is important to recognize, that data subject right to data portability should not \textit{adversely affect} the freedoms and rights of others (art. 20(4) GDPR). Due to the relatively broad scope of the provision, the transmission of personal data might in many cases have an impact on third parties as well.\textsuperscript{536} In some cases, datasets may include \textit{personal information of several individuals}. Despite the restrictive dimensions of the provision, data processors might not have to adopt an \textit{overly narrow} the scope of application, which according to the EC, also seems to include \textit{raw data} (EC Data Portability Guidelines, p. 7-9).

\textsuperscript{528} However, when the provision under art. 20 GDPR is applied, the transparency requirements and general obligations concerning the exercise of data subject rights shall also be taken into account (art. 12 GDPR).

\textsuperscript{529} Voigt 2017, p. 170.

\textsuperscript{530} In relation to the right to erasure (art. 17 GDPR), it should be noted that the transmission of data sets does neither entail the \textit{termination of the contractual relationship} between parties nor does it automatically include \textit{erasure} of the data by the controller. In other words, the data controller maintains control over the data sets concerning the data subject although means of data minimization may be required under art. 5(1) c GDPR (Voigt 2017, p 175).

\textsuperscript{531} Voigt 2017, p. 168-169 and 176. See also Janal 2017, p. 64.

\textsuperscript{532} See Fulford 2017 for the compliance aspects of the right to portability.

\textsuperscript{533} In the context of \textit{intellectual property rights} and \textit{trade secrets}, the use of this right may also have negative impacts on entities. For example, if the copyright protecting the software used by the controller is affected, the relevant information needs not to be transferred. Nevertheless, it seems unlikely that this exception could provide basis for a complete refusal for transmission of data. Instead, anonymization of data or limitation of data sets could be utilized in the transfer (Voigt 2017, p. 173).

\textsuperscript{534} Voigt 2017, p. 169-170. The writer mentions examples, such as profiling information and tracking data.

\textsuperscript{535} Scudiero 2017, p. 120.

\textsuperscript{536} Voigt 2017, p. 171.
interpretation of this right and would not be obliged to transfer data including information on third parties.\textsuperscript{537} For example, Voigt and Von dem Bussche argue that the practical impact of article 20 GDPR would be significantly weaker if a partial transfer of a user profile would reduce the potential for reuse of personal data.\textsuperscript{538}

\subsection*{5.1.2 Exclusion of the right to data portability}

Since article 20(1) GDPR requires that the data transmission between controllers takes place without hindrance, different technical measures hindering the transmission are to be considered unlawful.\textsuperscript{539} However, at the moment it is not clear whether this wording prevents a contractual exclusion of data portability. The GDPR itself does not provide rules on the lawfulness of contractual exclusions or restrictions of data subject rights. If the right to data portability is to be considered a specification of the art. 8 ECFR and art. 16 TFEU concerning individual’s right to data protection, it should be subject to strict limitations.\textsuperscript{540} Because the primary economic goal of data portability is to foster fair competition between services providers, it is obvious that the provision seeks to prevent lock-in situations in the market.\textsuperscript{541} The exclusion of this right might bind customers to their service providers, effectively preventing them to switch to another service provider.\textsuperscript{542}

In practice, individuals may lack the choice despite the legal protection under article 20 GDPR. Since many online services such as social networking platforms are benefitting from indirect network effects, and the multi-sided businesses often involve innovation, these industries seem to be prone to monopolization. This recent development trend may risk the individual control over personal data. In addition, consent to data processing by a monopoly can hardly be regarded as freely given.\textsuperscript{543} For example, as the report of the Belgian Data Protection Authority from 2015 states, Facebook was leveraging its dominant position on the online social networking market in order to legitimise the behavioural tracking of individuals across devices and services.\textsuperscript{544}

The fact that article 20 GDPR is only applied to personal data processing activities based on the data subject’s consent\textsuperscript{545} or on a contractual necessity\textsuperscript{546}, makes its scope of application relatively limited. Therefore, in situations where data processing is based

\begin{footnotesize}
\textsuperscript{537} EC Data Portability Guidelines, p. 7-8.
\textsuperscript{538} Voigt 2017, p. 172. It should be noted that also third-party information may sometimes be highly sensitive and the data processing entities should always evaluate the possible transfer risks on a case-by-case basis. The breach of article 20 GDPR can lead to fines of up to €20 million euros or up to 4% of the total worldwide annual turnover of the entity (art. 83(5) GDPR).
\textsuperscript{539} Article 20(1) GDPR and recital 9 GDPR.
\textsuperscript{540} Voigt 2017, p. 175-176. See also Gebicka 2014, p. 161-172.
\textsuperscript{541} For the definition of market lock-in, see section 4.2.6. See also Graef 2013C and Di Porto 2015, p. 298.
\textsuperscript{542} Voigt 2017, p. 176. As an important dimension of the information society, the Internet is considered a common good requiring that rights to data protection and privacy are respected. Data portability is therefore closely linked to the freedom to switch between networks without being constrained to a specific network (Hijmans 2016A, p. 91-92).
\textsuperscript{543} Lysnkey 2015, p. 263.
\textsuperscript{544} Van Alsenoy 2015B, p. 11.
\textsuperscript{545} Section 2.2.3.1.
\textsuperscript{546} Section 2.2.3.2.
\end{footnotesize}
on several legal grounds, it can be difficult to determine whether article 20 GDPR should apply. It should also be noted that the scope of the right to data portability as well as of other data subject rights can be limited under article 23 GDPR granting EU Member States broad competence for these national actions.

5.2 Abuse of dominance under Article 102 TFEU

5.2.1 The concept of abuse of dominance

As an important provision of the EU competition law, article 102 TFEU is directed towards the unilateral abusive acts and practices of dominant companies. Whereas its companion, article 101 TFEU, focuses on agreements between undertakings, article 102 TFEU is designed to deal with the abuse of substantial market power and monopoly behaviour of firms in a dominant position. It has to be noted that this provision only applies to the conduct of dominant undertakings, not to other anti-competitive practices used by these economic operators to achieve dominance. Article 102 provides:

“Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in:

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.”

The prohibited abusive acts and practices under article 102 TFEU can be roughly divided into exploitative and exclusionary abuses. The former refers to conduct whereby the dominant undertaking takes advantage of its market power and is therefore able to exploit its customers. An exclusionary abuse can be understood as

547 Voigt argues, that sometimes in circumstances described above, where the application of art. 20 GDPR is possible, it might be justified for the controller to contractually limit or exclude this right when considering the interests of all parties involved (p. 176).
548 Voigt 2017, p. 176. The scope of these national limitations under the GDPR is still rather unclear and will only be observed in practice.
549 Whish 2015, p. 183. In addition to the conduct of a single undertaking, article 102 TFEU can also be applied to collective dominance. However, this notion is not widely explored in the CJEU case law (see Case T-342/99 Airtours [2002], ECR II-02585 and Joined Cases C-68/94 and C-30/95 SCPA [1998], ECR I-01375). For the concept of abuse of dominance, see also Gerber 2017, p. 82-97.
550 Jones 2016, p. 258.
551 Several essential features of an abusive conduct can be distinguished from article 102 TFEU. These include for example: (1) the application of competition rules to undertakings (economic activities), (2) the effect on trade between Member States, (3) abusive conduct, (4) the dominant position held in a substantial part of the internal market, (5) abuse.
552 See Whish 2015, p. 212. The writer recognizes also a third group of abusive conduct, namely single market abuses. The concept refers to behaviour that is harmful to single market.
conducit preventing effective competition by excluding competitors from the market (forclosure).553

Traditionally, the abusive market behaviour has been defined by reference to competition on the merits.554 In the judgement Michelin I [1982], the Court of Justice linked the notion of abuse to methods differing from the ones used in normal competition. The assessment of these abusive methods was to be based on the traders’ performance.555 However, article 102 TFEU should not be interpreted in a way that contradicts article 101 TFEU. Too aggressive enforcement of the provision might, for example, punish the development of products superior to the competing products, effectively sheltering less efficient companies. Therefore, prohibiting or discouraging undertakings from competing actively ‘on the merits’ by means of enforcement might in practice lead to similar effects as cartels when competitors would be more protected than consumers.556

As price is not often a reliable indicator when measuring the substitutability in the online business environment, the competition is usually based on non-price elements, such as product quality. For this reason, this chapter focuses mainly on abusive non-pricing practices prohibited under article 102 TFEU.557 If a firm abuses its dominant position by refusing to share information with potential new market entrants, the weakened competition is likely to harm both competitors, and consumers as individuals. When discussing anti-competitive practices related to big data it is therefore important to analyse whether an above-mentioned decision of a dominant undertaking not to grant access to its datasets could constitute a refusal to deal under article 102 TFEU. If the answer is positive, the liability under the competition rules of the TFEU might lead to application of so-called essential facilities doctrine.558 This doctrine is related to a specific form of exclusionary anti-competitive behaviour. A typical example concerns an undertaking refusing to give access to a certain infrastructure or other essential facility crucial for competitors in order to be able to compete with the incumbent.559

5.2.1 Exclusionary non-pricing abuses under article 102 TFEU

Most frequently, article 102 TFEU is applied to exclusionary behaviour of undertakings.560 Many of the non-pricing strategies, aimed at raising rivals’ costs often

---

553 Jones 2016, p. 270.
554 See for example Case 85/76 Hoffmann-La Roche [1979], ECR 461, para. 91 and section 2.4.1 of the thesis.
555 Case 322/81 Michelin I [1983], ECR 03461, para. 70.
556 Waelbroeck 2010, p. 119.
557 See for example Whish 2015, p. 721-722. The concept of non-pricing practices can be understood encompassing for example exclusive dealing agreements, tying and refusals to supply. According to Whish, there is no legal significance in the division between pricing and non-pricing practices under article 102 TFEU as they both have similar anti-competitive effects.
558 The concept is further discussed in sections 5.2.2.1 and 5.2.2.2. See also section 3.3.1.2 (Potential competition and barriers of entry) and OECD 1996, p. 7-9.
559 Graef 2016A, p. 16.
560 The EC Guidance on Article 102 TFEU Enforcement Priorities provides useful aspects that the Commission considers important when investigating possible exclusionary abuse of dominance. See for
at the expense of consumers, are subtler than the ones involving pricing elements. In the early judgement C 6/72 Continental Can [1973], the CJEU stated that the provision could be applied to both exclusionary and exploitative abuses. It also clarified that the list of abusive conduct under article 102 TFEU is not exhaustive. Although a relatively old case, this judgement remains important to the law as it confirmed the broad applicability of the article 102 TFEU to abusive acts and practices.

Since abuse is an objective concept, the conduct infringing article 102 TFEU can be found although no causal link between the intention or fault of an undertaking and the consequences are found. The narrow application of the article would lead to decreased efficiency if competition authorities would only be focusing on practices resulting from the exercise of market power by a dominant firm. Although the CJEU noted in the judgement C-333/94 P Tetra Pak [1996] that the application of article 102 TFEU presupposed a link between the dominant position and the alleged abusive practices, this statement is not completely in parallel with the Continental Can. Instead of being interested in the use of market power, the CJEU wanted to assess whether the abusive conduct could take place in a market other than the one in which an economic operator was dominant.

In many cases, exclusionary practices are less risky for undertakings as they often involve entirely rational and lawful market behaviour. For example, defensive litigation is often a key strategy of a company protecting its commercial assets and fulfils its obligations towards its shareholders. Although there are myriad of different non-pricing strategies undertakings can use when unlawfully excluding their rivals, cases involving abusive non-pricing strategies have been relatively rare under article 102 TFEU.

Concerns about horizontal and vertical foreclosure may rise when a dominant undertaking is able to prevent new competing entrants from the market in an anti-competitive way. The foreclosure can occur both downstream and upstream in the market. For example, a vertically integrated company could harm competition on at either level of the market. Exclusionary abuses may also concern horizontal foreclosure such as purchasing agreements or predatory pricing. However, some of the non-pricing
strategies, such as refusal to supply, concern mostly anti-competitive effects in the downstream market.\textsuperscript{569}

5.2.2.1 Refusal to supply

As earlier mentioned, a dominant undertaking can infringe article 102 TFEU by refusing to grant access to its facilities or to supply its products or services.\textsuperscript{570} According to the EC Guidance on the Article 102 TFEU Enforcement Priorities, this act does not necessarily have to be actual, a constructive act of refusal is sufficient.\textsuperscript{571} However, unilateral refusals to supply by non-dominant companies do not fall within the scope of EU competition rules.\textsuperscript{572} Although a recognized form of abusive non-pricing practices prohibited under article 102 TFEU, the topic remains relatively controversial in competition law.\textsuperscript{573}

It should be noted that the duty to deal and supply is not a general obligation to assist competitors. For this reason, it can only be applied if the refusal would be likely to cause significant harm to competition.\textsuperscript{574} The input in question must also be an essential component in the relevant market for the final product.\textsuperscript{575} In the case judgement C-7/97 Bronner, the Advocate General Jacobs highlighted the fact that the primary purpose of article 102 TFEU was to prevent distortions of competition. In particular, the Advocate General considered the interests of consumers even more important than that of competitors.\textsuperscript{576} Therefore, an abusive act of refusal to deal should be regarded as an example of limiting production at the cost of consumers within the meaning of article 102(b) TFEU.\textsuperscript{577} The duty to deal with competitors and consumers is only relevant and necessary if the downstream market lacks the sufficient competitive conditions: it would not be rational to require such actions under article 102 TFEU. Another important prerequisite is that the obligation to grant access should increase competition instead of discouraging it. This is why consumer interests should be emphasized in the enforcement efforts. As this prohibition under 102 TFEU often interferes with basic property rights and inevitably affects the incentives to future

---

\textsuperscript{569} Whish 2015, p. 215-216.
\textsuperscript{570} According to Dethmers, refusal to supply is the most commonly found type of abuse prohibited under article 102 TFEU since it covers a broad range of anti-competitive practices (Dethmers 2017, p. 153-154).
\textsuperscript{571} EC Guidance on Article 102 TFEU Enforcement Priorities [2009], para. 79. The term constructive refusal refers to market behaviour of a company, such as imposing unfair trading conditions for the supply, unduly delay or degrading of the supply of the product in question and charging of unreasonable prices.
\textsuperscript{572} Jones 2016, p. 496. See Joined Cases C-2/01 and C-3/01 P Bayer [2003], ECR I-00023, para. 141.
\textsuperscript{573} Whish 2015, p. 737. Several arguments may speak against the requirement to deal with competitors or customers, for example the contractual freedom of competing undertakings and reasons related to economic welfare, intellectual property rights and dynamic efficiency.
\textsuperscript{574} Also other types of abusive conduct can in some cases be classified as refusal to supply. In the CJEU case 311/84 CBEM [1985], ECR 03261, the obligation to buy advertising time on television only from the television company's own sales agency was considered both a tie and a refusal to supply.
\textsuperscript{575} O'Donoghue 2013, p. 510. The EC Guidance on the Article 102 Enforcement Priorities [2009] discusses the concept of refusal in paragraphs 75-88. In addition, the European Commission has made several statements concerning this concept, for example in Case IV/34.689 Sea Containers v. Stena Sealink [1993], para. 66.
\textsuperscript{576} Opinion of the Advocate General in Case C-7/97 Bronner [1998], ECR I-07791, para. 58.
investments, some exceptional competitive harm and clear benefits to the duty arise.\textsuperscript{578}

The early judgement in joined cases 6/73 and 7/73 \textit{Commercial Solvents} [1974] was the first decision in which the potential anti-competitive effects of a \textit{vertical foreclosure} were acknowledged by the Court of Justice.\textsuperscript{580} In the case, an Italian pharmaceutical company using aminobutanol as an ingredient in its drugs, was refused supplies by the manufacturer of this raw material. After the customer company’s complaint, the European Commission had decided that the supplier firm was dominant in the market and had abused its position by refusing to supply the essential drug ingredient to its customer. This conclusion was supported by the fact that the supplier’s anti-competitive behaviour was also likely to lead to the elimination of a producer of aminobutanol-derivative products.\textsuperscript{581} According to the Court of Justice, the main factors leading to the finding of abusive behaviour were the \textit{abuse of dominance} in order to affect competition on the derivatives market, the supplier’s \textit{refusal to deal} with an existing customer when it intended to compete in the downstream market as well as the fact that the act of refusal could potentially eliminate its customer from this market.\textsuperscript{582} The dominant company, Commercial Solvents, had integrated vertically in order to gain competitive advantages. However, the Court of Justice neither discussed the potential efficiencies of this strategy, nor the possible benefits to consumers as end-users.\textsuperscript{583}

In order to be qualified as abusive behaviour, a refusal to supply must be related to an input \textit{indispensable} to carrying out an economic activity in the adjacent or downstream market.\textsuperscript{584} In addition, it seems to be easier to require a dominant company to supply others with a service or product already available on the market than with one previously only in its own use.\textsuperscript{585}

\textbf{5.2.2.2 The essential facilities doctrine in EU law}

Originating in US antitrust case law\textsuperscript{586}, the \textit{essential facilities doctrine} is closely linked to the assessment of article 102 TFEU and especially cases related to refusals to supply.\textsuperscript{587} Largely due to the relatively controversial nature\textsuperscript{588} of this principle, the

\textsuperscript{578} Case C-7/97 \textit{Bronner} [1998], ECR I-07791, paragraphs 39-40.
\textsuperscript{579} O’Donoghue 2013, p. 510.
\textsuperscript{580} Joined Cases 6/73 and 7/73 \textit{Commercial Solvents} [1974], ECR 00223.
\textsuperscript{581} Ibid., para. 49.
\textsuperscript{582} Ibid., para. 25.
\textsuperscript{583} Jones 2016, p. 499.
\textsuperscript{584} Incardona 2006, p. 350-351.
\textsuperscript{585} Hou 2016, p. 2. According to the writer, if a dominant undertaking is required to externalize a reserved product, this obligation is likely to alter both the \textit{commercial policy} of the company and the current \textit{market structure}.
\textsuperscript{587} Under EU competition law, abusive behaviour under the essential facilities doctrine can be understood as a special case of refusal to deal or supply (Bergman 2001, p 405). It has also been presented that the doctrine should be considered an \textit{additional refinement} to the principles under article 102 TFEU (Furse 1995, p. 472). See also EC Guidance on Article 102 TFEU Enforcement Priorities [2009], para. 78.
CJEU has preferred the term *indispensability* in its decisional practice. Usually the term refers to a situation in the downstream market where the competitors of a vertically integrated dominant undertaking need access to be able to provide products and services to their customers. However, it has to be remembered that the doctrine is neither a new nor distinctive concept concerning the application of article 102 TFEU. Instead, it is considered a term of classification for cases sharing the same characteristics. In these circumstances, the core question is whether a dominant firm controlling an essential facility can be forced to contract with its competitors.

The European Commission referred to the concept of essential facilities first time in 1992, in the decision *Sealink [1992]*. Although the case never went to a final decision and was eventually settled, it provided an early example of the assessment of essential facilities doctrine in the European context. The case concerned the owner and operator of a port in Wales. The EC considered the operator, Sealink Harbours, dominant on the market for port facilities for ferry services on the British side. A competing firm had complained to the commission that the introduction of a new ferry timetable by Sealink would cause disruption for the competitors in the port essential to their businesses. The Commission ordered Sealink to return to its previous timetable by Sealink would cause disruption for the competitors in the port essential to their businesses. The Commission ordered Sealink to return to its previous timetable stating that as the owner of an essential facility, it could strengthen its position in another related market by granting market access to its competitors on less favourable terms without an objective justification. This conduct was considered a breach of article 102 TFEU.

When considering the scope of the essential facilities doctrine, the CJEU judgement C-7/97 *Bronner [1998]* was of great significance as the Court sought to limit the circumstances in which it could be applied. The case concerned two competing newspaper publishers in Austria. The publisher with a significant market share, Mediaprint, had refused to grant its small-sized competitor Bronner access to its home-delivery scheme. However, another newspaper printed and distributed by Mediaprint was included in this scheme. In its decision, the CJEU considered the possible abuse

---

588 It has often been difficult to justify access to a facility on traditional infrastructural grounds (Frischmann 2008, p. 59). See also Hawker 1999, p. 122-128.
589 Jones 2016, p. 500. However, the General Court has used the term in several of its judgments, for example in Case T-374-375 European Night Services [1998], ECR I-03141, para. 191 and in Case T-52/00 Coe Clerici Logistics [2003], ECR II-02123, para. 62. See also the Opinion of Advocate General Jacobs in Case C-7/97 *Bronner* [1998], ECR I-07791, paragraphs 33 and 45-53 and Glasi 1994.
590 The term bottleneck monopoly is sometimes used synonymously. Essential facilities cases typically have a strong vertical element as the owner of the facility seeks to extract profits from the market on which the facility is sold or used (O’Donoghue 2013, p. 512).
591 O’Donoghue 2013, p. 510. See also the following cases involving essential facility elements: Case C-18/88 GB-Inno [1991], ECR I-01541 and Case T-504/93 Ladbroke [1997], ECR II-00923.
592 Case IV/34.174 *Sealink* [1992]. Jones and Suffrin argue that the rationale behind essential facilities doctrine could to some extent be found even in the early case law, such as the Continental Can. For the use of the concept, see also the following EC decisions concerning the airline industry and ports Case IV/32.318 *London-European Sabena* [1988] and Case IV/33.544 *British Midland v. Aer Lingus* [1992].
593 Case IV/34.174 *Sealink* [1992], paragraphs 41 and 42. See also Jones 2016, p. 501. For the application of the doctrine in EU, see Waller 2010, p. 745-752.
594 Whish 2015, p. 742. In its decision, the Court referred to the earlier IP-related case *RTE* (Joined Cases C-241/91 and C-242/91 P *RTE* [1995], ECR I-1743). *Evrand* considered Bronner as a catalyst for the application of the doctrine in EU law. The writer argues that the number of potential essential facilities in the European Union has significantly increased since the early 1990s Evrand 2004, p. 525).
595 Case C-7/97 *Bronner* [1998], ECR I-07791.
of dominant position under article 102 TFEU by Mediaprint and the essential nature of the home-delivery scheme in newspaper business. Avoiding the use of the term essential facilities, the Court of Justice listed four factors required to be present in order to the refusal to be considered an abuse. First, all competition had to be potentially eliminated by the act of refusal from the person requesting access. Secondly, the refusal could not be objectively justified. Thirdly, the access to the facility had to be indispensable in order to continue the other person’s business. And fourthly, no actual or potential substitute could exist.\textsuperscript{596}

In \textit{Bronner} judgement, these criteria were not met. Merely desirable or convenient access to a facility could not be regarded as indispensable within the meaning of article 102 TFEU. The CJEU also pointed out that the indispensability of the access required that it would not be economically viable to create a similar delivery system with a comparable circulation. Considering the status of Bronner as a small-circulation newspaper, the arguments concerning the abuse of dominance could not be supported.\textsuperscript{597} However, the judgement left several important questions unanswered. For example, the role of competition authorities in similar circumstances remained unclear.\textsuperscript{598}

The principles of assessment developed in the Commercial Solvents and Bronner cases have later been applied, for example, in the context of intellectual property rights, computer maintenance services and spare parts manufacturing and supply. In its judgement C-712/14 \textit{CEAHR v. Commission} [2017], the CJEU assessed a complaint against several Swiss watch manufacturers, such as Rolex and Swatch Group.\textsuperscript{599} The companies were alleged to have agreed on a concerted practice and abused their collective dominance by refusing to continue to supply spare parts to independent watch repairers.\textsuperscript{600} The European Commission had concluded that the market for the sale of watches sold at a price exceeding 1000 euros (so-called prestige watches) and the market for the supply of spare parts were separate and distinct from each other. In addition, it had found that there was only limited substitutability between repair services across brands. The selective repair system set up by the Swiss watch manufacturers allowed independent repairers to become authorized repairers if certain objective criteria were met. The EC stated that the watch manufacturers had not reserved the secondary markets to themselves by preventing the market entry of independent repairers. As the systems did not eliminate effective competition, the refusal could not be considered sufficient to establish the existence of abuse.\textsuperscript{601}

When assessing the second plea of the applicant CEAHR concerning the alleged abusive conduct, the CJEU answered to the question whether the Commission had made an error of assessment when identifying the necessary criteria to establish a prohibited conduct. The Court confirmed the Commission’s findings stating that the

\begin{itemize}
\item \textsuperscript{596} Ibid., para. 41.
\item \textsuperscript{597} Ibid., para 45-46.
\item \textsuperscript{598} Jones 2016, p. 506.
\item \textsuperscript{599} Case T-712/14 \textit{CEAHR v. Commission} [2017], ECLI:EU:T:2017:748.
\item \textsuperscript{600} Ibid., para. 2.
\item \textsuperscript{601} Ibid., paragraphs 16-18.
\end{itemize}
refusal to supply could, only in certain circumstances, constitute an abuse within the meaning of article 102 TFEU. Referring to the Commercial Solvents judgement, it continued that the systems did not eliminate effective competition. In order to be considered abusive, the refusal had to lack an objective justification and the conduct had to be likely to eliminate all competition on the part of the person requesting the goods and services. Therefore, the Court concluded that the Commission had correctly found that a refusal to supply could only exceptionally constitute an abuse prohibited under article 102 TFEU.602

In the recent years, the European Commission seems to have to some extent lightened the requirement concerning the elimination of all competition.603 In the decision Telekomunikacja Polska, the EC found that likely anti-competitive effects of a refusal to supply did not mean that competitors were actually forced to exit the market. A finding that rivals were obliged to compete less aggressively and their market positions were more disadvantageous was sufficient.604 Similarly, in the ENI decision, the Commission stated that the Bronner test was satisfied if the refusal was likely to result in either prevention or elimination of the development of effective competition on the downstream market.605

The principle of essential facilities should be applied carefully, since imposing a duty to deal or supply with competitors would significantly interfere with the economic rights of an undertaking.606 These public actions should only be justified when less intrusive measures would not be sufficiently effective. Therefore, it seems to be crucial to identify the elements making business assets actually ‘essential’ or ‘indispensable’ for competitors and customers. Issues, such as the terms of access, might be problematic if the parties seek to settle their own terms. The owner of the facility might be able to impose unfair terms for example with respect to prices.607 In contrast, if a public authority intervenes the contractual negotiations with the intention to unilaterally set the terms of supply, it may become a price regulator.608 In economic sectors where the construction of an essential facility does not include public funding, even greater caution should to be exercised since unjustified intervention would mainly do harm to the public interest and reduce consumer welfare by removing incentives to innovation.609

602 Ibid., paragraphs 87-91.
603 Jones 2016, p. 507.
604 Case COMP//39.525 Telekomunikacja Polska [2011], para. 815. The case was later upheld by the General Court (Case T-486/11 Orange Polska [2015], ECLI:EU:T:2015:1002). See also Kamiński 2011.
605 Case COMP/39.315 ENI [2010], para. 40. See also Case C-52/09 TeliaSonera [2011], ECR I-00527, para. 55.
606 For example, Lang 2017, p. 22-24.
607 See for example Case C-242/95 GT-Link [1997], ECR I-04449. In this case, the Court of Justice found that excessive duties imposed by a public undertaking on a ferry firm constituted a breach of article 106 TFEU, in conjuction with article 102 TFEU.
608 The difficulties in settling the terms of supply can be seen for example in the Case T-167/08 Microsoft [2012], ECLI:EU:T:2012:323.
609 Jones 2016, p. 503. See also Bergman 2000, p. 61.
5.2.2.3 Data as an essential facility

Even though an undertaking’s refusal to supply essential facilities has traditionally arisen in the context of physical infrastructures and assets protected by intellectual property rights, the increasingly digital business environment has raised questions about the applicability of the essential facilities doctrine to many multi-sided businesses using personal data, such as online platforms. Several official reports discussing the role of data as a competitive advantage have been issued over the past years. This is a clear indication of the importance of the topic and the emerging challenges digital markets are facing.

The use of algorithms is a central feature of the online platform businesses. They are used to collect relevant user data and improve the service quality on the user side of the platform. However, on the advertiser side the accumulating user data are monetized through different targeted advertising models, such as the pay-per-click model. Consequently, the expanding number of users also increases the revenues of the service provider. According to Graef, this phenomenon could be considered economies of scale in relation to the commercial use of data. The competitive strength of many digital businesses is closely related to the quality and amount of personal data that the companies hold. Due to the fact that certain types of data decline in value over time, it is important for market operators to continue their gathering and verifying activities. The turnover generated by a digital services provider through the monetization of data might indicate the competitive position of a firm in a potential market for a certain type of data. If there are no data-related revenues, potential competition may constitute sufficient indication of dominance in the relevant market.

Access to data may constitute a barrier to entry, but this finding requires that factual circumstances are taken into account. If partial substitutes for the essential datasets exist, the quality of this information determines whether it can be used by new market entrants in the launch of a new service. The European Commission has concluded in many of its earlier decisions involving big data aspects that access to user data is not likely to give a competitive advantage to the dominant companies effectively impeding effective competition. The reason for this has been the fact that similar information has already been available for competitors and out of the control of the dominant firm.

---

610 For example Graef 2011.
611 Graef 2016A, p. 245. See also Abramson 2014 and Colangelo 2017, p. 264-265.
612 See for example the following documents: EDPS Opinion Privacy and competitiveness in the age of Big Data 2014, Monopolkommission 2015 and CMA UK 2015. In 2016, the French Competition Authority launched its own sector inquiry concerning the online advertising industry and the significance of data processing for competition in that sector. See also Modrall 2017.
615 In many cases, it can be difficult to argue that access to context-dependent data generated by search engines could be considered absolutely indispensable (Argenton 2011, p. 17).
617 Ibid., p. 264-265. See for example the following decisions: Case COMP/M-4731 Google/DoubleClick [2008], paragraphs 365-366; Case COMP/38.784 Telefonica [2007], paragraphs 539-558 and Case COMP/M-7217 Facebook/WhatsApp I [2014], paragraphs 187-189.
Although it does not seem easy to consider a dominant firm’s data resources indispensable for the provision of targeted advertising services, the case might be different as regards the quality levels of services provided to users for example by many online platforms. Suggested social network interactions, relevance of search results and purchase suggestions in e-commerce platforms are examples of digital functionalities often requiring specific data not already available on the market.\textsuperscript{618} For instance, in the context of search engines, it is necessary for the maintenance of the good quality of service to obtain user data from a specific user. Third-party information does not form an adequate substitute for the search engine provider.\textsuperscript{619} From this point of view, competition authorities should to be able to investigate whether data are harmful to competition and consumer welfare.\textsuperscript{620}

Over the past years, the French and Belgian competition authorities have investigated abuse of dominance cases in which the key question has concerned the possibility of competing firms to reproduce datasets held by a dominant undertaking. Since both of the following cases included the cross-use of data developed in the context of monopoly, they might not be directly associated with the data-driven markets in which for example online platforms operate. However, both decisions included references to reasonable financial and temporal conditions in which potential competitors should be able to reproduce a database. This approach might also be relevant in the assessment of the indispensability of a dataset and the economic viability of duplication in the online business environment.\textsuperscript{621}

In 2014, the French competition authority (AC) adopted a decision concerning the French multinational electric utility company GDF Suez (known as ENGIE since April 2015).\textsuperscript{622} The AC found that GDF Suez had abused its dominant position in the natural gas market. The company had acquired these datasets because of its historical role as a nationalized gas monopoly.\textsuperscript{623} The intention of GDF Suez was to launch offers at market prices outside the scope of its position as a public service provider. The AC stated that the legality of these activities depended on the conditions in which the company had established its customer base. In addition, it had to be analysed whether equally efficient competitors could reproduce these datasets at reasonable financial conditions and in a timely manner.\textsuperscript{624}

The AC concluded that GDF Suez had not achieved its monopoly status as a result of a specific innovation it had developed by its own merit. It was equally clear that the competitors could not reasonably have relied on information of other databases or reproduced the same competitive advantage effective for attracting new customers in

\begin{footnotesize}
\begin{itemize}
    \item \textsuperscript{618} According to Stucke and Grunes, if data were freely accessible, online platform service providers would not be investing significant resources in the development of these free services (Stucke 2015, p. 7). See also Graef 2015B. For antitrust enforcement in e-commerce, see Henty 2017.
    \item \textsuperscript{619} Graef 2016A, p. 265.
    \item \textsuperscript{620} Song 2017, p. 670.
    \item \textsuperscript{621} Graef 2016A, p. 267.
    \item \textsuperscript{622} Decision No. 14-MC-02 of the French Competition Authority (L'Autorité de la Concurrence), 9.9.2014.
    \item \textsuperscript{623} Ibid., para. 100.
    \item \textsuperscript{624} Ibid. para. 146.
\end{itemize}
\end{footnotesize}
the market for gas supply.\textsuperscript{625} The company could have been able to foreclose potential competitors from the liberalized electricity and gas market. Therefore, Autorité de la concurrence stated that GDF Suez practices could be regarded as abuse of dominance under article 102 TFEU.\textsuperscript{626} It adopted interim measures necessary to restore market balance and ordered GDF Suez to suspend its commercial practices outside its public services obligation unless it had made the necessary datasets available to its competitors.\textsuperscript{627}

In 2015, the Belgian competition authority (ABC) investigated the alleged abuse of dominant position in the market for public lotteries by the Belgian National Lottery (\textit{Nationale Loterij NV}).\textsuperscript{628} As a public law limited company, Nationale Loterij had a legal monopoly in the market. The company decided to use its contact details when entering the competitive market for sports betting in 2013. This information was contained in a database that it had established as a legal monopolist and the intention was to use this personal data for promotional purposes when launching a new product.\textsuperscript{629} As in the case of GDF Suez, it was necessary to assess the circumstances in which the dominant company had established the database and the potential reproducibility of the database for the competitors. Given the size and nature of the database, it could not have been reproduced by the competitors of Nationale Loterij.\textsuperscript{630} Although the ABC followed the AC’s reasoning when assessing the criteria for the reproducibility of the database, it did not require Nationale Loterij to share the relevant personal data with its competitors in the sports betting market. Since the company only intended to use this information once in its campaign, a stricter intervention might have been disproportionate.\textsuperscript{631}

Opposite the aforementioned analysis, it seems possible that in certain circumstances data-driven companies may seek to exclude competitors from the market by restricting or preventing access to essential data resources. To some extent these acts and practices seem to be even natural if the business model of a company is solely based for example on the processing of personal data.\textsuperscript{632} In the online environment, the liability under article 102 TFEU would most likely emerge in the context of \textit{indirect competition}. In these circumstances, a new market entrant or potential competitor needs the data as an input for products or services not in direct competition with the incumbent firm. However, the special characteristics of data should always be taken into account when considering the applicability of the essential facilities doctrine. For example, big datasets can be non-rivalrous but still be made exclusive.\textsuperscript{633} Dominant companies could also invoke the obligations under EU data

\textsuperscript{625} Ibid., paragraphs 147-154.
\textsuperscript{626} Ibid., paragraphs 169-174.
\textsuperscript{627} Ibid., paragraphs 285 and 297.
\textsuperscript{628} Case PK-13-0012 \textit{Nationale Loterij NV}, 22.9.2015.
\textsuperscript{629} Ibid., paragraphs 44-48.
\textsuperscript{630} Ibid., paragraphs 69-70.
\textsuperscript{631} Graef 2016A, p. 267.
\textsuperscript{632} For example, Google has restricted the portability of advertising campaigns by demanding exclusivity agreements for search advertisements from websites (see for example Joaquín Almunia 2012, 26.11.2012).
\textsuperscript{633} The \textit{sui generis} nature of many legal regimes, such as database protection and trade secret law are of great importance from this point of view. These regimes do not impose \textit{qualitative requirements} for the subject matter of the protection (Graef 2016A, p. 274).
protection law in order to justify their refusal to grant access to personal data of their users. Therefore, it would be important for competition authorities to consider the interaction between data protection and competition law if a dominant firm’s duty to deal would eventually involve use of personal data.634

5.3 Applicability of EU competition rules to data portability

Compliance with the right data portability under article 20 GDPR requires significantadministrative efforts from the companies as they are expected to provide individuals their personal data in a transferable and usable format.635 It is also important to notice that article 20 GDPR addresses the matter of data portability from the perspective of individual users. For this reason, the emphasis of the right is not on the rights of businesses, such as direct competitors or other service providers. However, due to its great importance to all stakeholders in the digital economy, the provision itself cannot secure data portability rights and needs to be supplemented by relevant EU competition rules.636 On the other hand, especially new start-ups and SMEs might be negatively affected as their compliance requirements are likely to increase. This is partly due to the fact that the right to data portability applies to all data controllers, not only to the ones in a dominant position.637

In a healthy competitive environment, consumers should be able to switch their digital service providers and transfer their personal data accordingly. In this respect, the right to data portability is also at the heart of competition policy. Indeed, when preventing user lock-in situations and higher switching costs for consumers, article 20 GDPR seems to have a central role. A key concern is related to the portability of users’ search behaviours and histories. This question also seems to form an essential link between data protection and competition law. Vanberg argues that especially the controller-to-controller type of data portability should be considered crucial to safeguard the effective competition in platform based markets as well as to secure the data subject right to data portability. The fact that, in reality, the transferred personal data may not actually be utilised by other data controllers as a result of architectural and technical constraints, could support this argument.638

In practice, it may be difficult for companies to demonstrate the need to access the personal data resources of a dominant competitor, instead of developing their own equivalent database. The relatively restrictive applicability of the essential facilities

634 Graef 2016A, p. 273-274.
635 For example, Google already has its own data export service, Google Takeout. However, it is not completely clear whether users make use of this opportunity. In general, individual users may not be interested this often time-consuming and complex process (Vanberg 2017, p. 10).
636 Vanberg 2017, p. 2. However, critics argue that the traditional competition law metrics for measurement of market power in a relevant market cannot be effectively applied to online companies (for example, Van der Auwermeulen 2017, p. 62). See also Graef 2016B.
637 Urquhart 2017, p. 10. Mandating data portability requirements for SMEs can be problematic as these companies not likely to have significant market power and therefore the burden of compliance might be unreasonable in relation to the benefits. In addition, innovation activities of small companies may be discouraged (Swire 2013, p. 352).
doctrine does not make this task much easier. However, as the cases presented below seek to demonstrate, the growing interest of both European Commission and national competition authorities to investigate digital markets involving personal data processing may indicate that the number of these cases is likely to increase.

5.3.1 The EC investigations into Google

The administrative process concerning the European Commission’s competition investigation into Google was launched first in 2010, when several vertical search engine companies, such as Ciao, Foundem and ejustice.fr filed a complaint before the EC. All three complaints focused on the alleged abuse of dominance under article 102 TFEU. According to Google’s competitors, the company had favoured its own vertical search services at the expense of the rivals. For the purposes of this thesis, the focus will be on data portability issues concerning Google’s vertical search services, especially the business practices related to the Google Shopping service and the AdWords platform.

Since 2008, Google had been changing its business strategy to develop and expand its comparison shopping service. Instead of competing on the merits in the market for comparison shopping services, Google’s strategy relied on the company’s dominant position in general internet search services. According to the Commission, Google has systematically favoured its own comparison shopping services and simultaneously reduced the visibility of competing services providers.

In relation to data portability, the Commission was concerned about Google imposing contractual restrictions on software developers. The terms could potentially prevent these companies from offering tools that facilitate the data transfer from Google’s AdWords to other search advertising platforms. Such restriction was likely to lock-in online advertisers to Google’s facilities and simultaneously have an adverse effect on the competing platforms, such as Microsoft’s Bing. Most of the small and medium-sized companies were basically forced to use Google’s advertising platform since the recreation costs of an online advertising campaign are significantly high. In its Preliminary Assessment in 2013, the EC found that Google had infringed article 102 TFEU with several of different business practices, including with the contractual

---

639 Vanberg 2017, p. 11. The greatest obstacle in accusations based on the infringement of data protection law seems to be the establishment of a causal link to the dominant market position (Díaz 2017, p. 413).
640 Case AT.39740 Google Search (Shopping) [2017], paragraphs 38-43. See also Reyna 2017, p. 2-4 and Van Loon 2012, p. 16-19.
641 See EC Press Release 30.11.2010 and Vanberg 2017, p. 11. In addition to the alleged restrictions on the portability of online advertising data to competing online advertising platforms, the EC also started to investigate other alleged violations of article 102 TFEU. These accusations included obligations imposed on advertising partners as well as the use of third party content in order to restrict competition to the detriment of consumers. Bork et al. strongly disagree with this view (Bork 2012, p. 700).
642 AdWords is Google’s auction-based online search advertising platform.
643 EU Focus 358/2017, p. 3.
644 Case AT.39740 Google Search (Shopping) [2017], paragraphs 341-343.
restrictions on the management and transferability of online search advertising campaigns.

The Commission’s decision in the first of the three separate investigations concerning Google was given in June 2017. Google was found to be dominant in general search markets in the EEA since 2008, with the exception of Czech Republic where the dominance was established since 2011. Google’s search engine had also held high market shares during the investigated period in all of the EEA countries, mostly exceeding the level of 90%. Google had been taking advantage of the high barriers to entry to the search engine market and simultaneously profiting from the network effects, making its services more attractive as the number of consumers using them increased. By abusing its dominant position, Google was able to make significant profits at the expense of competing firms and to the detriment of European consumers. In the Google Search (Shopping) decision, Google was eventually fined €2.42 billion for abusing dominance as search engine.

In addition, the European Commission has already come to the preliminary conclusion that the company has abused its dominant position also in two other cases still under investigation. The Commission is concerned that Google has suppressed innovation and consumer choice in different mobile services by employing a strategy aimed at expanding its dominant position in the market for general Internet search services. Google is also accused to have prevented third-party websites from sourcing search advertisements from competing firms in relation to its AdSense service, consequently reducing choice.

The Google investigations seem to highlight the role of the European Commission in the efforts to facilitate data portability in the digital economy. The actions of the Commission may also be necessary when the potential consumer lock-in situations in the highly concentrated online platform markets are prevented. It is clear that as a dominant search engine operator, Google possesses large amounts of personal data in the form of search results, search behaviour and user search history. By refusing to

---

646 Case AT.39740 Google Search (Shopping) [2017], para. 63. As part of Google’s antitrust settlement with the US Federal Trade Commission, the company had agreed to change its Adwords API terms and conditions hindering data portability between service providers (see for example Google Letter 27.12.2012). However, the EC initiated antitrust proceedings against Google in 2016.
647 Case AT.39740 Google Search (Shopping) [2017].
648 Ibid., para. 271.
649 Ibid., para. 685.
650 Ibid., para. 314.
651 Ibid., p. 152-155. Since the start of the abusive conduct, the user traffic of its comparison shopping service had increased 45-fold in the UK, 29-fold in France and 35-fold in Germany, just to name a few.
652 Ibid., para. 754. See also EC Press Release 27.6.2017. Google and Alphabet, Inc. have brought an action concerning the Google Search (Shopping) decision (Case T-612/17, 11.9.2017).
653 See the following pending EC investigations into Google Search business: Case AT.40.411 Google Search (AdSense) and Case AT.40.499 Google Search (Android).
655 See EC Press Release 14.7.2016. This manipulative technique was not only discriminating competitors, but it was also likely to affect the quality of organic searches offered to its users (Chirita 2015, p. 122).
656 However, Daly argues that since Google only has to do relatively superficial changes to its practices and is not obliged to for example increase transparency as to its algorithm, the consumer benefits appear to be minimal (Daly 2017, p. 6).
share this valuable and often sensitive data with its competitors, the company is able to prevent other search engine operators to challenge its position in the market.\textsuperscript{657} It has even been argued that competing search engine platforms could provide search results of at least \textit{similar quality} to the consumers if Google were to grant access to search results.\textsuperscript{658}

The aforementioned concerns also reflect the fact that restrictions on the right to data portability may constitute an abuse of dominant position under article 102(b) TFEU. If so, it has to be proven that the dominant undertaking actually limits technical development and markets in general to the detriment of consumers.\textsuperscript{659} In addition, it is likely that article 102 TFEU could potentially expand the scope of the data subject right under article 20 GDPR. Although the latter provision protects the rights individual data subjects, the parallel application of article 102 TFEU could take into account the interests of businesses which normally would not be protected by the GDPR.\textsuperscript{660}

\textbf{5.3.2 The Facebook investigation in Germany [2016-2018]}

In 2016, the German Federal Cartel Office (\textit{Bundeskartellamt}) launched an investigation concerning FB’s usage of WhatsApp’s analytics and personal data resources. It was under suspicion that Facebook had abused its market power by infringing data protection rules.\textsuperscript{661} This case was the first time when a dominant undertaking was subject to a competition investigation concerning the alleged \textit{infringement of data protection laws}.\textsuperscript{662} With its specific \textit{terms of service}, the company could potentially use its dominant position in the \textit{market for social networks} and infringe article 102 TFEU. Therefore, it was possible that Facebook had imposed \textit{unfair conditions} on users by using unlawful contractual terms violating data protection provisions, if the consumers were not sufficiently informed of the nature and the extent of personal data collected.\textsuperscript{663} As previously discussed, the European Commission was at this point also investigating Facebook’s privacy policy and data protection practices.

There were several challenges that Bundeskartellamt had to deal with when gathering evidence for its conclusions. First, it had to be shown that Facebook was dominant in the separate social networks market. The definition of relevant market also seemed challenging when considering the possible restrictions of \textit{data portability} between service providers. The reason for this was the fact that Facebook did not

\textsuperscript{657} Vanberg 2017, p. 12. See also Sng 2017.
\textsuperscript{658} Lianos 2013A, p. 455. The writers distinguish three types of abusive behaviour arising from the discussion concerning Google’s business practices: \textit{strategies reducing multi-homing, leveraging} and \textit{exploitative practices}.
\textsuperscript{659} See for example Geradin 2013, p. 11.
\textsuperscript{660} Vanberg 2017, p. 12.
\textsuperscript{661} In her speech in January 2016, Competition Commissioner Vestager had already stated that the vast amounts of personal data collected by \textit{dominant technology platforms} could be considered violating EU competition rules if these big data sets were used as an entry barrier with the intention to drive competitors out of the market (Margarethe Vestager 17.1.2016).
\textsuperscript{662} Vanberg 2017, p. 13.
\textsuperscript{663} Bundeskartellamt 2.3.2016. See also Song 2017, p. 669-670.
directly compete with many social network service providers also exploiting personal data, such as Pinterest, LinkedIn or Snapchat. The previous incumbent in the market, Myspace, had already been swept away at this point. Secondly, it was not yet clear whether the company had abused its dominant position by the terms and conditions imposed on consumers. Tying together two more or less remote areas of law, such as data protection law and competition rules is not always an easy task, despite the fact that data are the main driver for many business models in the digital economy.664 

The third challenge Bundeskartellamt was facing in the case concerned the establishment of a causal link between the alleged violation of article 102 TFEU and the breach of data protection legislation.665 In 2013, the Federal Court of Justice of Germany (Bundesgerichtshof, BGH) had ruled in its decision KZR 58/11 concerning certain special payments made by the Retirement Fund of the Federal and State Government Employees that the illegal general terms and conditions set by a dominant undertaking could constitute an abuse of dominance under the German competition law. The prohibition of exploitative business terms was based on paragraph 19(2) No. 2 of the German Competition Act (GWB).666 Bundeskartellamt’s approach was based on this national judgement potentially providing the necessary connection between the two legal regimes.667

Interestingly, the 9th amendment of the German Competition Act came in to force in mid-2017.668 This amendment concerned specific internet-related criteria used in the assessment of market power in the digital economy. These new tools of competition assessment were also to be used when assessing the network effects and access to data issues. After the amendment, Bundeskartellamt was also given authority to investigate acquisitions of firms with only small turnovers but which are eventually purchased with a high price. Start-up mergers may often involve these elements. High purchase price may often serve as in indication of a valuable innovative business idea and the company’s high competitive potential.669

In its preliminary assessment in December 2017, Bundeskartellamt presented the findings concerning the admissibility of Facebook’s personal data processing terms.670 It stated that Facebook was dominant on the German market for social networks. It was also abusing this dominant position by making the use of its social network conditional and requiring consumers to allow Facebook’s limitless amassing of all user data generated by third-party websites, such as WhatsApp, Instagram or apps of other companies. According to the authority, the final decision in the case is not expected until early summer 2018.671

664 MacLeod 2013, p. 367.
665 Ibid., p. 368.
671 Ibid., p.1
According to Bundeskartellamt, Facebook as a social network operator had to consider the fact that the users of its services could not switch to other social networking platforms. Therefore, data portability seemed to be at the heart of this case as well. The German Federal Cartel Office considered the take-it-or-leave-it-style nature of Facebook’s trading terms were inappropriate, and they were also likely to violate data protection law to disadvantage of its users. It was equally uncertain whether Facebook as a dominant undertaking had acquired appropriate consent to the type of data processing and collection the company used in its business activities. The essential argument behind these findings was the will to give consumers more control over their personal data and for this reason, Facebook also had to give them reasonable options to limit the economic exploitation of their sensitive information. However, this investigation was limited to the user data collected from third-party sources, not from the Facebook’s own social network platform. Bundeskartellamt also left explicitly open the question if the latter data collection and processing activities also constituted abuse of dominance.

With its preliminary assessment notice, the German authority offered Facebook a possibility to comment and answer to the findings of Bundeskartellamt. Since the Facebook investigation was an administrative proceeding, the possible outcomes are the offer of commitments by the undertaking, the termination of the case or a prohibition by Bundeskartellamt.

The Facebook investigations of Bundeskartellamt clearly reflect the growing interplay between data protection concerns and EU competition law. The fact that Bundeskartellamt has closely co-operated with data protection authorities during the procedure also seem to underline this connection. The case also serves as an example of how the failure to comply with relevant provisions of the GDPR, for example article 20 GDPR, can potentially trigger competition law investigations at national or EU level. If the infringements of the GDPR are found to have adverse effects on consumers and harm competition within the EU, it is also likely that other dominant technology companies may also be in the line of fire as well.

5.4 The concept of fairness in the digital sector

5.4.1 The controversial nature of personal data

It is not always simple to approach issues related to the nature, use and protection of personal data. Many people seem to have considerably different values and understanding of data resources also referred to as “the new oil” of our economy. For

---

673 Ibid., p. 2.
674 Ibid., p. 2
678 See for example the former Commissioner for consumer protection Kuneva’s speech (Kuneva 31.33.2009, p. 2).
example, competition law professionals seem to be more reluctant to accept the synergies between different legal frameworks such as competition law, data protection law and consumer law, despite the fact that the EDPS has issued two opinions in this context.679 The interests related to effective innovation activities and different business strategies clearly differ from the ones emphasizing the protection of personal data as a profound and fundamental value of our society. Yet it seems to be important to seek fair balance between these often contradictory approaches stemming from the data-driven nature of the modern competitive markets.

In the digital context, the most prominent two-sided business strategies usually involve generation of revenues from user profiling and advertising. From the corporate point of view, the two-sided nature of many digital business models involves subsidizing the economic losses on one side of the market with more or less lucrative business practices on the other side.680 The accumulating personal data are likely to raise competition concerns since the market power of individual companies can substantially increase.681 Facebook’s recent acquisition of WhatsApp and the activities of Bundeskartellamt reflect the increasingly topical nature of these questions. Due to the relatively controversial nature of personal data, it seems to be important to consider what kind of market behaviour actually is fair in the digital economy.

Despite its common use, fairness as a concept is relatively flexible and can have different interpretations depending on the legal context. For example, the definition of fairness in the context of consumer law is not equivalent to its meaning in article 6 of the ECHR.682 However, underpinning equality, justice and democracy, it is an essential element of the modern European society.683 Nazzini distinguishes formal, substantial and procedural dimensions in the concept of fairness. The first dimension refers to the absence of discrimination or bias in the application of legal rules or the allocation of resources. In other words, fairness is seen as a process in which all participants are given equal opportunities. The substantial nature of fairness denotes the outcome of an allocation of resources. For example, if the resources are to be allocated between companies and consumers, the result should be fair. Procedural fairness reflects the nature of the market as the mechanism to allocate scarce resources. The market as such should not be distorted in favour of one economic operator and to the detriment of other stakeholders.684

In the context of EU data protection law, fairness can be understood reflecting the essential aim of the protection of individual control over personal data. This profound aspect was originally formulated in the practice of the German constitutional court.685

---

679 Ohlhausen 2015, p. 394. See also Kimmel 2014, p. 50, Pozzato 2014, p. 469-470 as well as EDPS Opinions 2014 and 2016. Since the administrative burden of competition authorities would be likely to increase, this critique appears to be somewhat natural.

680 Koops 2014, p. 251-252. The writer describes the nature of this business strategy with the term divide-and-conquer.

681 Kalimo 2017, p. 211.

682 Nazzini 2011, p. 21-22.

683 Through these fundamental values, it can also be understood reflecting the aims of article 2 TEU.

684 Nazzini 2011, p. 22.

685 Kalimo 2017, p. 314. The German Constitutional Court (Bundesverfassungsgericht, BVerfG) stated in its judgement in 1983, that privacy related issues "can be taken into account in the competition assessment
Fairness can also be seen supporting and pursuing the other objectives of data protection legislation, such as the balance between the rights and interests of data controllers and data subjects, or the prevention of power symmetries. According to the former EU Data Protection Supervisor Hustinx, these objectives are essential when securing the broader structural protection of individuals. Despite their somewhat overlapping nature, the individual’s control over personal data and the concept of fairness should not be considered mutually exclusive or contradictory. Instead, Kalimo argues that the requirement of individual control should be regarded as a precondition for achieving fairness as an overarching value of EU data protection law. For the aforementioned reasons, fairness in the context of EU data protection law could be described to be formal by nature.

The EU Courts, competition authorities and scholars have often considered the main objectives of competition law to be market integration, economic welfare and consumer protection. However, Ahlborn and Padilla divide competition law objectives to three different groups: fairness, market integration, and welfare and efficiency. In EU competition law, the concept of fairness appears mainly in its procedural and substantial form. Consequently, the notions of fair competition and fair market can be seen referring to equal opportunities of economic operators when competing to benefit from the market, both as buyers and sellers. Although the concept of fairness in the context of competition law remains relatively unclear, the development of the new digital market seems to require that fairness and economic welfare in general be taken into account in the competition considerations. Moreover, the EDPS stated already in 2014 that the development of online business models is likely to require the reformation of the legal concept of harm in order to reflect more effectively the potential breaches of data protection legislation. From this point of view, it could be possible to measure the harm or detriment caused by the market power of digital companies with non-economic considerations, such as data protection law and privacy. Therefore, fairness in the context of EU competition law represents a more indirect protection of privacy and personal data.

5.4.2 Fairness of personal data processing

Fairness as a concept is explicitly referred to in the legal instruments of the European Union. In addition its solid position in the article 8 ECFR, both the DPD and the

to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor” (15.12.1983, BVerfGE 65, 1-71, Volkszahlung).

687 Hustinx 2014, p. 17.
690 Ahlborn 2008, p. 61-62. In addition, the authors consider the fairness goals of competition law to be the following: fairness, the protection of rivalry and the competitive process, the protection of SMEs, and the protection of economic freedom.
692 Ibid., p. 24
693 EDPS Opinion 2014, p. 32.
694 Kalimo 2017, p. 315. The indirect effect of data protection considerations seem to be more significant in markets where data protection and privacy constitute the essential parameters of competition.
GDPR refer to fairness in their substantive provisions. The recital 38 of the DPD clarifies the notion of fairness by stating, that

“...the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing the circumstances of the collection.”

The term ‘accurate and full information’ may be understood as a necessary condition when securing fairness in data processing activities. Referring to details, such as the controller’s identity and further information necessary to guarantee fairness, article 10 of the DPD provides a detailed list of what could be regarded as such information.

The rapid technological development and the increasing exploitation of personal data by companies may create new risks in the context of data protection efforts. Moreover, Maxwell argues that the nature of these challenges and potential harm to consumers are still poorly understood. Since the essential aim of the GDPR is answer to these challenges by guaranteeing a high level of data protection, strengthen online privacy and boost the digital economy of the EU, fairness is also present in the substantive provisions of the Regulation. As an example, article 5(1)(a) of the GDPR refers to fairness of data processing alongside the general principles of transparency and lawfulness. Despite the similarities of these two legal instruments, it should be noted that unlike the DPD, the General Data Protection Regulation treats the principles of transparency and fairness as separate obligations. This could be an indication of the increasing importance of fairness as a value in EU data protection law.

5.4.3 The requirement of consent and unfair digital trading terms

A company processing personal data fairly has to have a legal justification for its data processing activities. Therefore, a specific, informed and freely given consent obtained from the data subject (art. 6(1)(a) GDPR) is often an essential element of fair personal data processing. In the context of competitive markets, consent is also an important requirement for the data-related commercial transactions between undertakings. Although it is somewhat unclear what fairness means under article 102 TFEU, it has been described as a two-dimensional concept encompassing horizontal and vertical aspects. In general, ‘fairness’ could refer to fair behaviour towards consumers, competitors and trading partners. In the context of article 102 TFEU, it should be considered unfair if a dominant undertaking would abuse its market power

---

695 Ibid., p. 316.
696 Maxwell 2013, p. 205.
697 Recitals 6 and 7 GDPR and Kalimo 2017, p. 316.
698 Recital 39 of the GDPR provides further clarification for example by stating that the specific purposes of personal data processing have to be determined at the time of the collection and the justifications must be explicit and legitimate.
699 Kalimo 2017, p. 316. See also Maxwell 2013, p. 208.
700 See also articles 2(h) and 7(a) DPD.
in order gain economic profits at the cost of consumers and competitors or by blocking the access from potential market entrants. In this respect, the unfair conduct seems to be equivalent to *anti-competitive behaviour*.\(^\text{702}\)

Abusive conduct harming consumers *directly* has traditionally received only limited attention in EU Competition law and for this reason, also the EC Guidance on Article 102 TFEU Enforcement Priorities is mainly focused on exclusionary practices.\(^\text{703}\) However, as many digital companies are using large amounts of personal data in their business activities, the prohibition of unfair conduct towards consumers under article 102(a) TFEU seems to be increasingly topical. In addition, the Competition Commissioner Vestager highlighted this concern in her speech in November 2016 when she referred to dominant businesses exploiting their customers by imposing *unfair terms*.\(^\text{704}\)

*Unfair trading terms* have not often been referred to in the decisional practice of the EU Courts and the European Commission.\(^\text{705}\) One of the first instances when the Court of Justice interpreted alleged unfair trading conditions was the judgement 127-73 SABAM [1974] concerning exploitation of copyrights.\(^\text{706}\) The Court associated the concept of fairness with the term *necessity*, even in its absolute form. It stated that the trading terms were considered unfair when a dominant undertaking exploited copyrights by imposing obligations that were not absolutely necessary in order to attain their *actual objective*. Moreover, these activities undermined the freedom to exercise copyright.\(^\text{707}\) From the general EU case law concerning the fairness of trading terms and conditions, it can be concluded that the concept is determined as a *set of factors or values* instead of being understood as a single defining feature.\(^\text{708}\) The concept of fairness has also been described being an umbrella notion relying on the contextual circumstances of the case in question.\(^\text{709}\)

Considering the relationships between companies processing personal data and digital consumers in the digital marketplace, it is clear that the special characteristics of this digital environment differing from more traditional offline trading conditions have to be taken into account. It should also be determined whether the business model and relations surrounding user profiling and advertising can be understood falling within the scope of article 102(a) TFEU. There are no explicit consensus on whether provision of digital services in exchange for the data subject’s consent for

---

\(^{702}\) Akman 2012, p. 149. Article 102(a) also refers to fairness when introducing a prohibition to directly or indirectly impose *unfair* purchase or selling prices or other *unfair* trading conditions.

\(^{703}\) Kalimo 2017, p. 318.

\(^{704}\) Margarethe Vestager 21.11.2016.

\(^{705}\) Kalimo 2017, p. 317. In addition, the previous references have been criticized to be more or less *imprecise and vague* (Cseres 2011, p. 427).

\(^{706}\) Case 127-73 SABAM [1974], ECR 00313.

\(^{707}\) Ibid., para. 15. For the interpretation of unfair trading conditions, see also the following cases: Case C-247/86 Alsatel [1990], ECR 05987, para. 10 and Case C-385/07 Duales System Deutschland [2009], ECR I-06155, para. 32.

\(^{708}\) Kalimo 2017, p. 319.

\(^{709}\) Akman 2012, p. 157. In their efforts to define *fair market conduct*, the EU authorities have used concepts and principles, such as *equality*, *proportionality*, *balance of interests*, *transparency*, *necessity*, *certainty* and *objectivity* (p. 156).
data processing constitutes a *contractual relationship*. However, it is obvious that these practices are *commercial* by nature and also the primary incentive for companies to enter into the personal data related transactions with users.

When approaching fairness of personal data trading terms from the competition law perspective, article 102(a) TFEU might be applicable and necessary to take into account. If the company provides *unclear, misleading or even deceptive information* concerning data-related conditions of the service, the terms of service could be problematic. As a result, consumers may not be able to understand or evaluate the conditions they are accepting. The competition and consumer-related concerns were partly dealt in January 2018, when the District Court of Berlin ruled that Facebook’s use of personal data was illegal. The company had not adequately ensured the informed consent of its customers, which was therefore declared invalid. Although the alleged illegal activity concerned a breach of German consumer law, several of Facebook’s personal data practices could also be interpreted in the context of data protection and competition law as well.

The Federation of German Consumers Organization (VZBV) had claimed that some of the company’s *terms of service and default settings* denied consumers a *meaningful choice* over the use of their sensitive information. The Court held Facebook’s terms of use also to be invalid. The firm had *pre-formulated* declarations of consent allowing Facebook to transfer the acquired user data, such as the name and profile picture to the USA. These personal data trading conditions also gave the firm the right to use personal data for *sponsored, commercial or related content*. The District Court of Berlin stated clearly that such pre-formulated declarations could not constitute *effective consent* to the use of personal data. However, VZBV did not succeed in its argument against Facebook’s claim that the *use of the company’s service is free of charge*. This question was significant when considering the great value of personal data for online platforms, such as Facebook. The District Court found that *intangible consideration* could not be considered a *cost*. According to VZBV’s press release, the organization intends to appeal to the Berlin Court of Appeal on the points rejected by the District Court. In turn, Facebook has stated that it already has made significant modifications to its privacy policy and terms of service and will seek to comply with the relevant provisions of the new GDPR.

---

710 Kalimo 2017, p. 319.
711 According to Solove, the transactions based on the exchange of personal data could be understood as *information trade* (Solove 2001, p. 1448).
712 See for example article 7(1) of the *Unfair Commercial Practices Directive*, which states that a commercial practice should be considered misleading and consequently unfair, if “it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise”.
713 Bundeskartellamt 2.3.2016. Kalimo’s reasoning follows a similar pattern (p. 319-320).
714 Landgericht Berlin 16.1.2018 (in German).
716 Verbraucherezentrale 14.2.2018, p. 32, B.B.4. (in English). This conclusion seems to some extent reflect the spirit of the recital 43 GDPR, according to which “in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, --”.
In the light of the analysis and comments made above, it is important to notice the overlap and interplay between different EU law regimes when assessing the possible breaches related to the competitive markets of the EU. Despite the relatively flexible and adaptive nature of EU competition rules, it seems unlikely that the emerging competition and consumer protection concerns in the digital economy could be answered solely by using the methods and tools provided by traditional methods of competition law. For example, the substantial limitation to users’ informational self-determination raises inevitably questions whether data protection and privacy considerations should be more distinctly present in competition assessment. Since the District Court of Berlin rejected the arguments of VZBV concerning the users paying with data for the use of Facebook’s services, the traditional approach to personal data as a competitive asset was not changed. However, since the process is likely to continue, a potential change in this interpretation is highly possible.
6 CONCLUSIONS

The collection, storage and analysis of vast datasets are essential features of many digital business models in the data-driven economy. Rising together with related technologies, such as Artificial Intelligence and the Internet of Things\textsuperscript{718}, big data and big analytics are undoubtedly the new drivers of economic growth also in the European Union. At the same time, the rapid technological development has significantly increased the complexity of personal data transfer, storage and collection activities in the digital environment. Therefore, one of the essential aims of the new European data protection legislation is to ensure a sufficient level of control over this informational expansion.\textsuperscript{719}

Finding a fair balance between effective data-based innovation and a sufficiently high level of personal data protection is often considered a major challenge for the European data protection framework. However, the applicability of the new data protection rules will be challenging especially in the digital context. As this thesis has sought to demonstrate, the GDPR has left several still unclear or otherwise abstract rules and definitions that might create data protection risks until the courts and developing case law limit the legal interpretation in the upcoming years. The disunity of legal interpretation is also likely to enable companies to benefit from the most favourable terms in their business practices.\textsuperscript{720} This fact might be to some extent in contradiction with the rights and reasonable expectations of consumers as individual data subjects.

Because the economic exploitation of personal data has clearly increased the value of personal information as a competitive asset, the risks related to abusive business practices are also evident. As illustrated in the thesis, the competitive strength of many digital businesses is in connection with the quality and amount of personal information these firms hold. Especially the emerging issues concerning article 20 GDPR and the right to portability have revealed the need for further analysis and development of the competitive concerns related to this notion and to its applicability. Because the balance of bargaining power is not always equal between the digital companies exploiting personal data and the users of their services, efficient protection mechanisms should be ensured in order to ensure the sufficient level of informational self-determination.\textsuperscript{721} This is crucial since the users’ security and privacy can be threatened due to their limited control, retention and choice over the collection and distribution of personal data.\textsuperscript{722}

\textsuperscript{718} According to Drexl, the major technological challenges of the IoT are related to big data analytics (Drexl 2017, p. 266). For the importance of big data in online platform competition, see Lerner A.V. 2014.
\textsuperscript{719} The size of the fines available to Data Protection Supervisory Authorities may indicate the growing importance of national DPAs in the enforcement efforts. Although significant economic sanctions for abuse of dominance or cartel activities have long been essential features of competition law enforcement, comparisons can be drawn with the GDPR (see for example Corbet 2016, p. 13-14, Albrecht 2016, p. 289 and Grac-Aubert 2015, p. 5-6). For the roles and powers of national DPAs, see Giurgiu 2016 and Hijmans 2016B.
\textsuperscript{720} Voigt 2017, p. 136.
\textsuperscript{721} See recital 43 GDPR referring to the imbalance of power between the data subject and the controller.
\textsuperscript{722} See for example Maras 2015, p. 99-104.
It is clear that the better and higher personal data protection within the EU will increase the administrative burden of data processing entities and require significant resources for the regulatory compliance. Nevertheless, considering the fact that personal data related business practices are often highly lucrative for economic operators, it is not unfair or disproportionate to argue that the compliance efforts and the costs they may create for companies are in many ways necessary and objectively justified. After all, setting the emphasis solely on the economic efficiency considerations would be likely to undermine the importance of personal data protection as a fundamental right of the European Union. However, rather one-sided approach to these issues is surprisingly common. In addition, the importance of personal data in the business practices of data processing entities and potential abusive behaviour are often underrated. Since many of the previous dissertations concerning this topic seem to have focused mainly on the competitive importance of data for economic operators, the essential aim of this thesis has been to provide a more versatile approach to this increasingly topical theme.

Since fair competition between economic operators and fair commercial practices are preconditions for the well-functioning single market of the European Union, it is important to take into account the potential for anti-competitive and unfair commercial practices in the digital sectors of economy. Like all other undertakings, companies operating in the digital marketplace are also bound by the rules of competition law. However, it seems unlikely that the emerging risks for fair competition in the digital marketplace could be sufficiently tackled with traditional methods of competition assessment. The discussion in chapters 4 and 5 has indicated that both merger activities of companies and their digital trading practices within the EU involve significant features related to commercial use of personal data. This study has sought to illustrate the fact that digital business strategies may involve abusive elements. Indeed, unilaterally formulated digital trading terms, increasing market concentration in many digital sectors and the potential lack of fairness in digital business practices are examples that highlight some of the legal challenges in the digital business ecosystem. Without an adequate level of personal data protection and sufficient enforcement efforts, it seems likely that the underlying principles of European data protection law may be at risk of being overshadowed by the rent-seeking activities of private entities.

---

723 For example, Von dem Busche 2016, p. 576-581. The writer argues that with the new data protection rules, obtaining consent will become more difficult.
724 Byers 2015.
725 See for example Zarsky 2017, p. 996. In the context of EC’s Google Search (Shopping) case, Broos and Ramos see Google’s role rather as a ‘matchmaker’ in search business than a dominant undertaking abusing its market position (Broos 2015, p. 2).
726 The arguments for the parallel application of EU law regimes and overlapping nature of competition law, consumer law and data protection legislation could be supported by the CJEU case C-32/11 Allianz Hungária [2013], ECLI:EU:C:2013:160. As an important outcome of this judgement, a breach of another area of law could be considered relevant when identifying a possible violation of competition law. (paragraphs 41 and 47). In the judgement, the CJEU emphasized the importance of domestic insurance law when identifying a competitive restriction under art. 101 TFEU (for example, Burnside 2015, p. 5).
727 As an example of the efforts to increase co-operation between European agencies from the different areas of law, the EDPS Giovanni Buttarelli called for the establishment of a “digital clearinghouse” developing guidelines that reflect the essential aims of different EU law regimes (EDPS Digital Clearinghouse). See also Bamberger 2017, p. 40.
**SVENSK SAMMANFATTNING**

**Introduktion**


Trots att många digitala tjänster i en datadriven ekonomi skenbart är kostnadsfria för konsumenter, är det klart att samling, förvaring och analysering av personuppgifter utgör en viktig konkurrenssfördel för många privata enheter i det digitala företagsekosystemet. Det är därför viktigt att notera att skyddet för personuppgifter också ska anses som en grundläggande rättighet skyddad av EU:s rättighetsstadga. Det växande ekonomiska utnyttjandet av stora datamängder i den digitala marknaden skapar också risker gällande EU:s konkurrenslagstiftning, och i synnerhet med tanke på digitala plattformar så som sociala nätverkstjänster, elektronisk handel och sökmotorföretag. Eftersom marknadskoncentrationen är relativt hög i många digitala sektorer, kan potentiella konkurrenxbegränsningar förekomma.

I artikel 20 i GDPR införs enskildas rätt till dataportabilitet. Regleringen strävar till att skydda och förstärka individens kontroll över sina personuppgifter, och strävar till att förbättra konkurrensvillkoren och ekonomisk tillväxt på EU:s inre marknad. Dataportabiliteten kan trots det vara problematisk speciellt beträffande fördraget om Europeiska unionens funktionssätt (FEUF) artikel 102, som förbjuder missbruk av dominerande marknadsställning. Om det är nödvändigt för konkurrerande tjänsteföretag att ha tillgång till personuppgifter, kan affärsclimatet bli ohållbart, ifall ett dominerande företag kan införa oskäliga avtalsvillkor eller använda orättvisa handelsmetoder för att utesluta konkurrenter eller försvåra tillgång till dessa nödvändiga nytting. Eftersom maktförhållandena och förhandlingskraften mellan personuppgiftsansvariga databehandlande enheter och individuella datasubjekt inte
alltid är jämna, kan det uppstå risker gällande dataskyddet. Exempelvis har den registrerade personen inte alltid haft möjligheten att ge sitt frivilliga, specifika, informerade och otvetydiga samtycke till behandlingen av sina personuppgifter enligt artikel 6(1) i GDPR. Dessa utmaningar illustreras delvis av de senaste juridiska oklarheterna och tvivel gällande Facebooks efterlevnad av EU:s lagstiftning om dataskydd och integritetsskydd, samt Europeiska kommissionens undersökning om Googles marknadsbeteende och verksamhet som en söktjänst.

**Motivering av studien och syftesformulering**


Eftersom de nya digitala företagsmodellerna i allt högre grad bygger på behandling av personuppgifter, kan den snabba utvecklingstakten skapa nya risker och äventyra den grundläggande rätten till skyddet för personuppgifter. Därför strävar avhandlingens första forskningsfråga till att förklara och granska reformen av EU:s skydd för personuppgifter och de framväxande utmaningar som den högre och allt mer omfattande dataskyddsnivån står inför, främst i förhållande till en rättvis konkurrens inom de datadrivna marknaderna. Trots GDPR:s allmänna målsättningar, är det ändå viktigt att notera att till exempel tonvikten i GDPR artikel 20 främst ligger på individens skydd och integritet, inte på företagssektorns ekonomiska rättigheter.

Avhandlingen strävar till att förklara framväxten av och risker gällande dataskydd och betydelsen av big data för digitala affärsmönster i konkurrenshänseende, främst i fråga om digitala plattformar. Fast den nya dataskyddsförordningen strävar till att ge enskilda personer mer kontroll över sina personuppgifter, har den teknologiska utvecklingstakten på många sätt överstigit genomsnittkonsumentens förståelse. GDPR
tillämpas på stora datamängder så fort de innehåller personuppgifter. Därför är det viktigt att kunna säkerställa att både privata och offentliga aktörer bär sitt ansvar och sin skadeståndsskyldighet gällande relevanta datarelaterade aktiviteter. Att följa GDPR:s grundläggande principer kräver ändå ofta mycket resurser och betydande ansträngningar från dessa databehandlande enheters sida. Delvis på grund av detta har dataskyddsreformen också kritiserats.

I studien presenteras några av de viktigaste digitala affärsmodellerna, nämligen sökmotorförgetag, plattformar för elektronisk handel och sociala nätverkstjänster. En central egenskap av dessa flersidiga affärsmodeller är den växelverkan de skapar mellan olika användargrupper. Många av de digitala tjänsterna så som serviceplattformar erbjuds tydligt kostnadsfritt för konsumenterna. Detta faktum kan vara problematiskt i synnerhet med hänsyn till Europeiska kommissionens kontroll av företagskoncentrationer, eftersom det inte med traditionella metoder är möjligt att definiera den relevanta marknad, som Kommissionens konkurrensrättsliga bedömning baserar sig på.

De mest framstående digitala affärsstrategierna på den digitala marknadsplatsen gäller speciellt användarprofilerering och riktad reklam. Trots att den ena sidan av marknaden skulle vara kostnadsfri för konsumenterna, är det viktigt att förstå att de ackumulerade personuppgifterna från användarsidan kan utgöra en vinstbringande inkomstkälla för ett digitalt företag. Därför klargör den tredje forskningsfrågan också risker som uppkommer gällande dataskyddsregleringen och konkurrensrättslig kontroll. De senaste utvecklingstrenderna i Europeiska kommissionens kontrollpraxis antyder att de traditionella tröskelvärdena för omsättning inte alltid fångar upp företagskoncentrationens verkliga betydelse, speciellt om transaktionen omfattar datarelaterade tillgångar eller andra resurser såsom företagets marknadsnärvägar och innovation. Eftersom graden av marknadskoncentration inom många digitala företagssektorer är framstående, borde konkurrens mellan tjänsteleverantörer säkerställas.

Den fjärde forskningsfrågan granskar faktorer som påverkar företagets marknadsskraft inom den digitala ekonomin. Fast det inte är enkelt att definiera en relevant marknad för informationshandel utan särskilda priser, är det klart att behandling och utnyttjande av personuppgifter i digital affärsverksamhet är av kommersiell natur. Marknadsandelar indikerar inte alltid effektivt företagens marknadsinflytande om marknaderna kännetecknas av snabb teknologisk förändring eller tillväxt. Därför skulle
det vara fördelaktigt att använda mera framåtblickande metoder vid bedömningen av en relevant marknad och av ett särskilt företags marknadskraft.

Avhandlingen förklarar också de potentiella konkurrensrättsliga risker som överträdelser av artikel 20 i GDPR kan orsaka både för de konkurrenskraftiga marknaderna och de registrerades rättigheter. Då man eftersträvar en rationell balans mellan olika intressen, som ofta varierar radikalt i diskussionen om behandling av personuppgifter och den nya dataskyddsregleringen på den digitala marknadsplassen, blir tolkningen av begreppet rättvisa centralt. Trots att begreppet varierar inom olika rättsområden, skulle det vara viktigt att bestämma hurdant marknadsbeteende egentligen kan anses vara rättvist. På detta sätt är personuppgiftsbehandlingens karaktär mycket kontroversiell. Eftersom dataskyddsrelaterade argument traditionellt inte har betraktats som en del av en konkurrensrättslig bedömning av EU-domstolen och Europeiska kommissionen, är många av avhandlingens teser också relativt framtidsorienterade och rentav spekulativa.

Den sista forskningsfrågan i studien syftar till att förklara i vilken omfattning det finns en grundläggande koppling mellan EU:s dataskyddsreglering och konkurrensrätt. Båda rättsområdena strävar till att förbättra marknadssintegration och individens välfärd. Digitaliseringen har skapat nya utmaningar för dataskydds- och konkurrensmyndigheterna. Därför är det viktigt att fundera på betydelsen av det växande samspelet mellan olika EU-rättsliga områden för att kunna förstärka och bibehålla allmänhetens förtroende för EU:s dataskyddspolicy samt att göra EU:s digitala marknader effektivare.

**Val av metoder, material och tidigare forskning**

Den allmänna dataskyddsförordningen träder i kraft i maj 2018. Därför är avhandlingen till sin natur också relativt framtidsinriktad vilket påverkar valet av metoder, material samt tillgängligt tidigare forskningsmaterial. I avhandlingen används relevant akademisk litteratur, de senaste publikationerna och kommentarerna i ämnet samt EU-domstolens rättspraxis, information från Europeiska kommissionen, vissa rättsfall från EU-medlemsstater och de nationella konkurrensmyndigheternas administrativa beslut. Eftersom EU:s tidigare dataskyddsdirektiv härstammar från år 1995, kommer också den personuppgiftsrelaterade EU-rättspraxisen från en relativt kort tidsperiod. Delvis på grund av den allmänna dataskyddsförordningens moderna
karaktär är också den tidigare forskningen inom avhandlingens område begränsad. Trots att den konkurrensträttliga forskningen och tillämpningen av EU:s konkurrensregler haft en stark roll inom Unionens ekonomiska politik redan över 50 år, märker man utifrån EU:s rättspraxis att myndigheterna och domstolarna fortsätter att klargöra väldigt grundläggande frågor, såsom tolkningen av etablerade begrepp. Det finns dock ännu viktiga tolkningsfrågor som förblir obesvarte.

Den juridiska argumentationen är huvudsäkrligen begränsad till Europeiska unionen, trots att många av de ämnen som diskuteras i avhandlingens mer eller mindre är gränsöverskridande och även omfattar andra ekonomiska samarbetsområden. Till exempel principen om nödvändiga nyttigheter har ursprungligen utvecklats i amerikansk rättspraxis och så småningom också etablerats i europeiskt bruk. Dessutom har många av de behandlade rättsfallen en internationell dimension eftersom den digitala ekonomin är alltmer global. Den Europeiska unionen kan på många sätt anses ha spelat en pionjärroll i utvecklingen av skydd av personuppgifter skydd och dessa synpunkter beaktas i allt större omfattning inom EU. Trots detta kräver många av de personuppgiftsraterade frågorna en bredare synvinkel och inställning. Då de asiatiska tillväxtnivåerna blir viktigare i förhållande till Europeiska unionen, blir också GDPR:s extraterritoriella räckvidd allt mer aktuell. För att kunna behandles avhandlingens forskningsområde tillräckligt omfattande är det därför viktigt att kunna förstå de olika dimensionerna och den betydelse som personliga data har och det stora värde som digitalt lagrad personlig information har som en affäristillgång inom den digitala ekonomin.

Avhandlingen är både praktiskt och teoretiskt inriktat. Trots att EU-domstolens och konkurrensmyndigheternas praxis används i form av en fallstudie för att stödja analysens juridiska argumentation, innehåller speciellt kapitel 3 relativt många teoretiska begrepp samt relativt mycket analys och granskning. I synnerhet konkurrensproblemen relaterade till big data och dataskyddsregler kräver i viss utsträckning en teoretisk infallsvinkel. Med en normativ inställning till vissa centrala principer och bestämmelser i den allmänna dataskyddsförordningen, syftar den första delen av studien till att bygga en stadig grund för den mer praktiska bedömningen och analysen av de personuppgiftsraterade konkurrensproblemen i avhandlingens andra del. Ett grundläggande metodologiskt mål i studien är med andra ord att undersöka, bedöma och även förutse vissa utmaningar som digitaliseringen skapar och som EU:s dataskyddsätt, konkurrensträtt samt de relevanta myndigheterna kommer att ställas
inför i framtiden. Som en följd av studiens framtidsinriktade natur, framlägger avhandlingen också vissa *de lege ferenda*-debatter gällande den senaste europeiska dataskyddsreformen. Dessutom innehåller avhandlingen också flera tekniska och icke-juridiska begrepp, vilka förklaras vidare i det inledande första kapitlet. Dessa begrepp är centrala för förståelsen av avhandlingens syfte och forskningsfrågor.

Avhandlingens struktur och redogörelse för genomförandet av undersökningen

Denna forskning har genomförts nära ikraftträdandet av EU:s allmänna dataskyddsförordning. Som ovan konstaterades, har studiens framtidsinriktade natur märkbart påverkat både det praktiska genomförandet samt avhandlingens utformning och struktur. Efter en grundlig källforskning, inblick i dokumentation och planmässig disposition, framskred avhandlingsprojektet relativt jämnt och inom den planerade tidsgränsen.

Eftersom insamling, behandling och kommersiellt utnyttjande av personuppgifter är centrala element i många digitala affärsmodeller, är det nödvändigt att diskutera några valda begreppsmässiga aspekter, centrala definitioner och GDPR:s bestämmelser innan man tar en mer praktisk inriktning och analytisk synvinkel till avhandlingens forskningsproblem. I detta sammanhang strävar avhandlingen att i kapitel 2 närma sig den europeiska dataskyddsreformen från ett normativt perspektiv.

Kapitel 3 granskar några av konkurrenssrättens viktiga begrepp och doktriner i ljuset av EU-domstolens rättspraxis och Europeiska kommissionens beslut. Efter inledningen, där några av de viktigaste digitala affärsmodellerna presenteras, diskuteras nyckelbegrepp i förhållande till FEUF artikel 102, som förbjuder missbruk av dominerande marknadsställning på EU:s inre marknad. Viktiga definitioner såsom relevant marknad, marknadskraft och potentiell konkurrens förklaras, och vidare diskuteras de digitala och datadrivna marknaderna. Bland annat dessa begrepp samt Europeiska kommissionens relativt framåtblickande och preventiva inställning gällande företagskoncentrationer, kräver delvis ett teoretiskt ramverk för att på ett grundligt sätt kunna svara på avhandlingens syftesformulering.

Marknadskoncentrationen i många digitala sektorer tenderar att vara relativt hög. Således ligger fokus i kapitel 4 på att granska utnyttjandet av big data, affärsstrategier och företagens beteendemönster bakom datadrivna företagskoncentrationer samt på
att identifiera potentiellt personuppgiftsrelaterat missbruk och konkurrensvillkor. I kapitlet diskuteras särskilt de dataskydds- och personintegritetsrelaterade hot och utmaningar, som dessa transaktioner kan medföra. Eftersom många av de senaste dataskyddsfrågorna inom EU gäller digitala plattformar, diskuteras utmaningen att definiera branschen, i synnerhet med hänsyn till Europeiska kommissionens senaste beslutspraxis.


Kapitel 6 strävar till att sammanfatta avhandlingens materiella bedömning och rättslig argumentation. Avsnittet återkommer till forskningsfrågor som presenterats i det inledande första kapitlet och redogör studiens viktigaste dragna slutsatser.

**Resultat och slutsatser**

Det främsta syftet i kapitlen 2 och 3 är att beskriva några av de huvudkoncept och rättsliga regler som berör undersökningens forskningsmål, samt att förklara den logiska grunden bakom Europeiska unionens dataskyddssystem och konkurrensvillkortliga system. Avhandlingen förklarar också den historiska bakgrunden till och utvecklingen av den europeiska dataskyddsregleringen, eftersom det annars inte är möjligt att fullständigt förstå den interna logiken och de rättsliga värden som skyddas med denna reglering. I många fall kan de varierande och ofta motstridiga
intressena i förhållande till behandling av personuppgifter orsakas av bristfällig information gällande lagstiftningens bakgrund och syfte.

Mot den historiska bakgrunden och utvecklingen av skyddet för personuppgifter i EU, är det inte alltid lätt att förutse vilken inverkan bestämmelserna i den allmänna dataskyddsförordningen har i verkligheten och på skyddsnivån. Den nya GDPR kan anses ha skapat flera oklara eller på andra sätt abstrakta formuleringar. Trots att förordningens ordval delvis strävar till att svara på de nya digitala utmaningarna inom ekonomin, krävs det större ansträngningar för att kunna uppnå en effektiv efterlevnad av EU:s dataskyddsreglering. Fast de behandlade datamängderna blir allt större, borde man inte bortse från kraven på en adekvat europeisk skyddsnivå för personuppgifter. I sista hand är det inte bara fråga om konkurrenskraftiga tillgångar av dataorienterade företag utan också grundläggande rättigheter som Europeiska unionen skyddar och erkänner.


Trots personuppgiftsbehandlingens relativt kontroversiella natur i den offentliga diskussionen, är det klart att de växande datamängderna samt värdet och rollen av personuppgifter inom de datadrivna industrierna kommer att kräva allt mer omfattande samarbete mellan de relevanta tillsynsmyndigheterna i EU. Denna ekonomiska dimension av personliga data skapar också den centrala länken mellan den
Europeiska dataskydds- och konkurrensreglering som också undersöks i denna avhandling.

Trots att Europeiska kommissionen traditionellt varit mycket tveksam till att ta ställning till dataskyddsaspekterna i sin övervakning av företagskoncentrationer, kommer avhandlingen fram till slutsatsen att tolkningslinjen har utvecklats mot en mer flexibel riktning. Detta argument kan anses vara trovärdigt när man beaktar den senaste dataskyddsutvecklingen i Europa i samband med digitaliseringen samt de senaste administrativa undersökningarna och rättsprocesserna gällande internetföretaget Googles söktjänster och den sociala nätverkstjänsten Facebooks efterlevnad av dataskyddsregler och integritet. Det har till och med påståtts att insamling av stora mängder data skulle leda till ett orättvist och orealistiskt inträdeshinder för nya marknadsaktörer.

I ljuset av avhandlingens analys, är det klart att de digitala marknadernas egenskaper skiljer sig från traditionella marknadens egenskaper på många sätt. När det gäller företagskoncentrationer, borde man notera att transaktionens målföretag kan ha relativt liten omsättning som inte tillräckligt indikerar den informativa potentialen och betydelsen av en särskild koncentration. Trots att EU:s konkurrensrättsliga regler är av en relativt flexibel och anpassningsbar karaktär, kan den traditionella konkurrensrättsliga inställningen och de omsättningsbaserade tröskelvärdena inte isolerade svara på alla aktuella utmaningar som digitaliseringen i Europa har skapat och kommer att skapa gällande rättvisa konkurrensvillkor, skyddet för personuppgifter och konkurrensövervakning i allmänhet.

EU:s allmänna dataskyddsförordning strävar generellt att på ett adekvat sätt kontrollera risker samt att sätta rimliga gränser för den datarelaterade expansionen den digitala ekonomin. Det är högst sannolikt att den mer omfattande och högre skyddsnivån av personuppgifter i Europa kommer att öka den administrativa bördan av databehandlande enheter och kräva större insatser för efterlevnaden av dataskyddsbestämmelserna. Å ena sidan kan det förefalla problematiskt eftersom big data och metoder för analys av stora datamängder är obestridligt de nya drivkrafterna i det digitala företagsekosystemet. Men eftersom personuppgiftsrelaterade affärsstrategier kan vara högst vinstgivande för dataorienterad affärsverksamhet, kan man med god rätt hävda att dessa ansträngningar och åtgärder är nödvändiga och objektivt motiverade. Ensidig betoning av personuppgiftsbehandlingens ekonomiska och affärsrelaterade dimensioner skulle lätt kunna leda till att den grundläggande
Europeiska rättigheten till personuppgiftsskydd ifrågasätts. På detta sätt handlar frågan bakom denna hetsiga debatt egentligen om definitionen och omfattningen av dataskyddsnivån inom EU:s inre marknader.
LIST OF REFERENCES

Literature


Argenton, Cédric; Prüfer, Jens: Search Engine Competition with Network Externalities, TILEC Discussion Paper, April 2011 (Argenton 2011)


Bapat, Anita: *The new right to data portability*, Privacy & Data Protection 13(3), 2013, p. 3-4 (*Bapat 2013*)

Batchelor, Bill; Allgrove, Ben; Agnew, Mark: *Digital disruption: the practical implications of the EU’s digital single market agenda*, European Competition Law Review 2015, p. 1-10 (*Batchelor 2015*)


Berendt, Bettina; Günther, Oliver; Spiekermann, Sarah: *Privacy in E-Commerce: Stated Preferences vs. Actual Behaviour*, Communications of the ACM, Vol. 48 No. 4, Pages 101-106 (*Berendt 2005*)


Bevitt, Ann; Dietschy, Laura: *GDPR series: the risks with data profiling*, Privacy & Data Protection 2016, 17(2), p. 6-8 (*Bevitt 2016*)


Blume, Peter: *The Data Subject*, European Data Protection Law 4/2015, p. 258-264 (*Blume 2015*)


Broos, Sébastien; Ramos, Jorge Marcos: *Google, Google Shopping and Amazon: The Importance of Competing Business Models and Two-Sided Intermediaries in...*, Technical Report, December 2015 (Broos 2015)


Bräutigam, Tobias: *Getting High on Information?* Tidsskrift utgiven av Juridiska Föreningen i Finland (JFT) 5/2012, p. 415-435 (Bräutigam 2012)


Böröcz, István: *Risk to the Right to the Protection of Personal Data: An Analysis*


Carlton, Dennis W.; Perloff, Jeffrey M.: Modern Industrial Organization, Pearson/Addison Wesley, 2005 (Carlton 2005)

Cate, Fred H.; Mayer-Schönberger, Viktor: Notice and consent in a world of Big Data, International Data Privacy, 2013, Vol. 3, No. 2 (Cate 2013)


Cowen, Tim: *Big Data as a Competition Issue: Should the EU Commission’s Approach Be More Careful*, European Networks Law and Regulation Quarterly (ENRL), Vol. 4, Issue 1, 2016, p. 14-23 (*Cowen 2016*).


Custers, Bart; Uršič, Helena: *Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection*, International Data Privacy Law 2016, Vol. 6, No. 1 (*Custers 2016*).


De Hert, Paul; Papakonstantinou, Vangelis; Malgieri, Gianclaudio; Beslay, Laurent; Sanchez, Ignacio: *The right to data portability in the GDPR: Towards user-centric


Den Hertog, Johan: *General Theories of Regulation*, Economic Institute / CLAV, Utrecht University (Den Hertog 1999)


Doherty, Calum; McLean, Fiona; Van Der Merwe, Danielle: *GDPR series: the new data subject rights*, Privacy & Data Protection 2017, 17(8), 9-11 (Doherty 2017)


Fulford, Nicola; Oastler, Krysia: *GDPR series: the new right to data portability*, Privacy & Data Protection 17(3), 2017, p. 3-6 (*Fulford 2017*)


Gebicka, Aleksandra; Heinemann, Andreas: *Social Media & Competition Law*, World Competition 37, no. 2 (2014), p. 149-172 (Gebicka 2014)


Geradin, Damien; Kuschewsky, Monika: *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, February 12, 2013 (Geradin 2013)


Graef, Inge: *Data as an Essential Facility: Competition and Innovation on Online Platforms*, KU Leuven, Faculty of Law, 2016 (Graef 2016A)

Graef, Inge: *Data Portability at the Crossroads of Data Protection and Competition Policy*, Big Data E Concorrenza, 9 November 2016, Roma (Graef 2016B)


Hemstruwer, Yoan: *Contracting around Privacy: The (Behavioural) Law and Economics of Consent and Big Data*, 8 JIPITEC 2017, 9, para 1 (Hemstüwer 2017)


Hou, Liyang: *Refusal to Deal within EU Competition Law*, Shanghai Jiao Tong University, June 11, 2010 (Hou 2010)

Hou, Liyang: *The Essential Facilities Doctrine – What Was Wrong in Microsoft?* International review of industrial property and copyright law, March 2012 (Hou 2012)


Jones, Alison; Sufrin, Brenda: *EU Competition Law: Text, Cases, and Materials*, Oxford University Press, 2016 (Jones 2016)


Kamiński, Damian; Rogzińska, Anna; Sasinska, Beata: Telekomunikacja Polska Decision, competition law enforcement in regulated markets, Competition Policy Newsletter 3, 22.6.2011 (Kamiński 2011)


Kiss, Attila; László Szőke, Gergely: Ecolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation, in Gutwirth, Serge; Leenes, Ronald; De Hert, Paul: *Reforming European Data Protection Law*, Springer 2015 (Kiss 2015)


Korah, Valentine: *Concept of a dominant position within the meaning of article 86*, in Greaves, Rosa: *Competition Law*, Taylor and Francis 2017 (Korah 2017)

Kuner, Christopher; Cate, Fred H.; Millard, Christopher; Svantesson, Dan Jerker B.: *The challenge of ‘big data’ for data protection*, International Data Privacy Law, 2012, Vol. 2(2) (*Kuner 2012*)

Kuner, Christopher; Cate, Fred H.; Millard, Christopher; Svantesson, Dan Jerker B.; Lynskey, Orla: *When two worlds collide: the interface between competition law and data protection*, International Data Privacy Law, 2014, Vol. 4, No. 4, p. 247-248 (*Kuner 2014*)


Körber, Torsten: *Common errors regarding search engine regulation - and how to avoid them*, European Competition Law Review 2015, 36(6), p.239-244 (*Körber 2015*)


Lerner, Andres V.: The Role of "Big Data" in Online Platform Competition, Compass Lexecon, August 26, 2014 (Lerner A.V. 2014)


Lundqvist, Björn; Forsberg, Ylva; De Vries, marc; Maggiolino, Mariateresa: Open Data and Competition Law_Some issues regarding access and pricing of raw data, Masaryk University Journal of Law and Technology, Vol. 9, Issue 2, 2015, p. 95-120 (Lundqvist 2015)


Maggio, Elena: *The competitive dynamics of app distribution platforms: to be or not to be open? Part 2*, European Competition Law Review 2017, p. 1-14 (Maggio 2017A)


Malgieri, Gianclaudio; Custers, Bart: *Pricing privacy – the right to know the value of your personal data*, Computer Law & Security Review 2017 (Malgieri 2017)


Monti, Giorgio: *The Concept of Dominance in Article 82*, European Competition Journal 2, p. 31-52 (*Monti 2006*)


O'Donoghue, Robert; Padilla, Jorge: *The Law and Economics of Article 102 TFEU*, Hart Publishing 2013 (O'Donoghue 2013)


Ohlhorst, Frank: *Big Data Analytics: Turning Big Data into Big Money*, John Wiley & Sons, Inc. (Ohlhorst 2012)


Paez, Mauricio; La Marca, Mike: *The Internet of Things: Emerging Legal Issues for Businesses*, 43 Northern Kentucky Law Review 29, 2016 (Paez 2016)

Picker, Randal C.: *Competition and Privacy in Web 2.0 and the Cloud*, Journal Articles, University of Chicago Law School, 2008 (Picker 2008)


Raitio, Juha: Euroopan unionin oikeus, 2016, Alma Talent, Talentum verkkokirjahylly, electronic version (Raitio 2016)


Santucci, Gérald: Paper for the International Conference on Future Trends of the Internet – From Internet of Data to Internet of Things, 28 January 2009 (Santucci 2009)

Savin, Andrej: Data Protection and privacy, in Savin, Andrej: EU internet law, Edward Elgar Publishing 2017 (Savin 2017)

Sayers, Samantha; Drury-Smith, James: GDPR series: how to operationalise profiling for your organisation, Privacy & Data Protection 2016, 17(1), p. 3-6 (Sayers 2016)


Shackleford, Scott J; Raymond, Anjanette; Danuvasin, Charoen; Balakrishnan, Rakshana; Dixit, Prakhar; Gjonaj, Julianna; Kavi, Rachith: When Toasters Attack: A

Shakila-Bu-Pasha; Alén-Savikko, Anette; Mäkinen, Jenna; Guinness, Robert; Korписаари, Päivi: EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency, European Data Protection Law Review 3/2016, p. 312-323 (Shakila-Bu-Pasha 2016)


Shapiro, Carl; Katz, Michael L.: Technology Adoption in the Presence of Network Externalities, Princeton University, 1986 (Shapiro 1986)


Sng, Yi Heng Alvin: Tying conduct under article 102 TFEU: can intervention against Google be justified? European Competition Law Review 2016, p. 1-10 (Sng 2016)

Sokol, Daniel; Comerford, Roisin: Antitrust and Regulating Big Data, Geo. Mason L. Rev. 23, 2016, p. 1129-1161 (Sokol 2016A)


Stigler, G.J.: Barriers to entry, economies of scale and firm size, in Stigler, G.J.: Organisation of Industry, Irwin 1968 (Stigler 1968)


Stucke, Maurice E.; Grunes, Allen P.: Big Data and Competition Policy, Oxford University Press 2016 (Stucke 2016)

Swire, Peter; Liagos, Yianni: Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Public Law and Legal Theory Working Paper Series, No. 204 (Swire 2013)


Treacy, Bridget; Bapat, Anita: *The "internet of things” – already in a home near you?* Privacy & Data Protection 2013, 14(2), p. 11-13 (Treacy 2013)


Urquhart, Lachlan; Sailaja, Neelima; McAuley, Derek: *Realising the right to data portability for the domestic Internet of things*, Springer 2017 (Urquhart 2017)

Ustaran, Eduardo: *EU General Data Protection Regulation: Things you should know*, Privacy & Data Protection 2016, 16(3), p. 3-5 (Ustaran 2016)

Van Alsenoy, Brendan; Koekkoek, Marieke: *Internet and jurisdiction after Google Spain: the extraterritorial reach of the ‘right to be delisted’*, International Data Privacy Law, 2015, Vol. 5(2) (Van Alsenoy 2015A)

Van Alsenoy, Brendan; Heyman, Rob; Verdoordt, Valerie; Ausloos, Jef: *From social media service to advertising network – A critical analysis of Facebook’s Revised Policies and Terms*, Working Paper, August 2015 (Van Alsenoy 2015B)


Whish, Richard; Bailey, David: Competition Law, Oxford University Press 2015 (Whish 2015A)


Zwitter, Andrej: *Big Data Ethics*, Big Data & Society 1/2014, University of Groningen Faculty of Law Research Paper (*Zwitter 2014*)

Case law (CJEU)


Case 127-73 Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior, 27.3.1974, ECR 00313 (*SABAM*)


Case C-85/76 Hoffmann-La Roche & Co. AG v Commission of the European Communities, 13.2.1979, ECR 1979 00641 (*Hoffmann-La Roche*)

Case 77/77 Benzine en Petroleum Handelsmaatschappij BV and others v Commission of the European Communities, 29.6.1978, ECR 01513 (*BP v Commission*)

Case 22/78 Hugin Kassaregister AB and Hugin Cash Registers Ltd v Commission of the European Communities, 31.5.1979, ECR II-01869 (*Hugin Kassaregister*)

Case 322/81 NV Nederlandsche Banden Industrie Michelin v Commission of the European Communities, 9.11.1983, ECR 03461 (*Michelin I*)
Case 311/84 Centre belge d'études de marché - Télémarketing (CBEM) v SA Compagnie luxembourgeoise de télédiffusion (CLT) and Information publicité Benelux (IPB), 3.10.1985, ECR 03261 (CBEM)


Case 247/86 Société alsacienne et lorraine de télécommunications et d'électronique (Alsatel) v SA Novasam, 5.10.1988, ECR 1988-05987 (Alsatel)

Case 53/87 Consorzio italiano della componentistica di ricambio per autoveicoli and Maxicar v Régie nationale des usines Renault, 5.10.1988, ECR 06039 (Renault)

Case 238/87 AB Volvo v Erik Veng (UK) Ltd, 5.10.1988, ECR 06211 (Volvo v Veng)


Joined Cases C-241/91 P and C-242/91 P Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities, 6.4.1995, ECR I-00743 (RTE)

Case C-53/92 P Hilti AG v Commission of the European Communities, 2.3.1994, ECR I-00667 (Hilti)

Joined Cases C-68/94 and C-30/95 French Republic and Société commerciale des potasses et de l'azote (SCPA) and Entreprise minière et chimique (EMC) v Commission of the European Communities, 31.3.1998, ECR I-01375 (SCPA)

Case C-333/94 P Tetra Pak International SA v Commission of the European Communities, 14.11.2996, ECR I-05951 (Tetra Pak)

Case C-242/95 GT-Link A/S v De Danske Statsbaner (DSB), 17.7.1997, ECR I-04449 (GT-Link)

Case C-7/97 Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, 26.11.1998, ECR I-07791 (Bronner)

Case C-450/00 Commission of the European Communities v Grand Duchy of Luxemburg, 4.10.2001, ECR I-07069 (Commission v Luxembourg)

Joined Cases C-465/00, C-138/01 and C-139/01 Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk, 20.5.2003, I-04989 (Rundfunk)

Joined Cases C-2/01 P and C-3/01 P Bundesverband der Arzneimittel-Importeure eV and Commission of the European Communities v Bayer AG, 6.1.2004, ECR I-00023 (Bayer)

Case C-101/01 Criminal proceedings against Bodil Lindqvist, 6.11.2003, ECR I-12971 (Lindqvist)

Case C-36/02 Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundestadt Bonn, 14.10.2004. ECR I-09609 (Omega Spielhallen)

Case C-418/01 P IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG [2004], 29.4.2004 ECR I-05039 (IMS Health)

Case C-238/05 Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc), 23.11.2006, ECR I-11125 (Asnef-Equifax)

Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU, 29.1.2008, ECR I-00271 (Promusicae)

Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, 16.12.2008, ECR I-09705 (Huber v Germany)

Case C-518/07 European Commission v Federal Republic of Germany, 9.3.2010, ECR I-01885 (Commission v Germany)

Case C-553/07 College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 7.5.2009, ECR I-03889 (Rijkeboer)

Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 16.12.2008, ECR I-09831 (Satamedia)

Case C-385/07 Der Grüne Punkt - Duales System Deutschland GmbH v Commission of the European Communities, 16.7.2009, ECR I-06155 (Duales System Deutschland)

Case C-28/08 P European Commission v The Bavarian Lager Co. Ltd, 29.6.2010, ECR I-06055 (Bavarian Lager)

Case C-52/09 Konkurrensverket v TeliaSonera Sverige AB, 17.2.2011, ECR I-00527 (TeliaSonera)

Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, 9.11.2010, ECR I-11063 (Schecke and Eifert)

Case C-34/10 Oliver Brüstle v Greenpeace eV, 18.10.2011, ECR I-09821 (Brüstle)

Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24.11.2011, ECLI:EU:C:2011:771 (SABAM)

Case C-209/10 Post Danmark A/S v Konkurrencerådet, 26.5.2012, ECLI:EU:C:2012:172 (Post Danmark I)


Case C-461/10 Bonnier Audio AB and Others v Perfect Communication Sweden AB, 19.4.2012, ECLI:EU:C:2012:219 (Bonnier)

Joined Cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, 24.11.2011, ECLI:EU:C:2011:777 (ASNEF)

Case C-32/11 Allianz Hungária Biztosító Zrt. and Others v Gazdasági Versenyhivatal, 14.3.2012, ECLI:EU:C:2013:160 (Allianz Hungária)

Case C-1/12 Ordem dos Técnicos Oficiais de Contas v Autoridade da Concorrência, 28.2.2013, ECLI:EU:C:2013:127 (OTOC)

Case C-56/12 European Federation of Ink and Ink Cartridge Manufacturers (EFIM) v European Commission, Lexmark International Technology SA, 19.9.2013, OJ C 344, 23.11.2013, p. 20-20 (EFIM)

Joined Cases C-141/12 and C-372/12 Minister voor Immigratie, Integratie en Asiel (C-372/12) v Minister voor Immigratie, Integratie en Asiel (C-141/12), Ms (C-372/12), 17.7.2014, OJ C 315, 15.9.2014, p. 2-3 (M)

Case C-291/12 Michael Schwarz v Stadt Bochum, 17.10.2013, ECLI:EU:C:2013:670 (Schwartz)

Case C-293/12 Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12), 8.4.2014, OJ C 175, 10.6.2014, p. 6-7 (Digital Rights Ireland)

Case C-351/12 Krajský soud v Plzni, 24.7.2012, OJ C 295, 27.2.2014, p. 5-6 (OSA)

Case C-473/12 Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte, 7.11.2013, OJ C 9, 11.1.2014, p. 13–14 (Englebert)

Case C-486/12 proceedings brought by X, OJ C 45, 15.2.2014, p. 13–14 (X)

Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů, 11.12.2014, OJ C 46, 9.2.2015, p. 6-6 (Ryneš)

Case C-615/13 P ClientEarth and Pesticide Action Network Europe PAN Europe) v European Food Safety Authority, 16.7.2015, ECLI:EU:C:2015:489 (ClientEarth)
Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), 7.7.2014, OJ C 212, 7.7.2014, p. 4–5 (Google Spain)

Case C-342/12 Worten - Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), 30.5.2013, ECLI:EU:C:2013:355 (Worten-Equipamentos)

Case C-201/14 Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others, 1.10.2015, ECLI:EU:C:2015:638 (Smaranda Bara)

Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, 1.10.2015, ECLI:EU:C:2015:639 (Weltimmo)

Case C-362/14 Maximillian Schrems v Data Protection Commissioner, 6.10.2015, ECLI:EU:C:2015:650 (Schrems)

Case C-373/14 P Toshiba Corporation v European Commission, 20.1.2016, ECLI:EU:C:2016:26 (Toshiba)

C-582/14 Patrick Breyer v Bundesrepublik Deutschland, 19.10.2016, ECLI:EU:C:2016:779 (Breyer)

Case C-191/15 Verein für Konsumenteninformation v Amazon EU Sàrl, 28.7.2016, ECLI:EU:C:2016:612 (Amazon EU)

Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, 9.3.2017, ECLI:EU:C:2017:197 (Salvatore Manni)

Case C-13/16 Valsts policijas Rīgas reģionā pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", 4.5.2017, ECLI:EU:C:2017:336 (Rīgas satiksme)

Case C-179/16 F. Hoffmann-La Roche Ltd and Others v Autorità Garante della Concorrenza e del Mercato, 23.1.2018 (Hoffmann)

Case C-248/16 Austria Asphalt Gmbh & Co OG v Budeskartellanwalt, 7.9.2017 ECLI:EU:C:2017:643 (Austria Asphalt)

Case C-73/16 Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy, 27.9.2017, ECLI:EU:C:2017:725 (Peter Puškár)
Case C-434/16 Peter Nowak v Data Protection Commissioner, 20.12.2017, ECLI:EU:C:2017:994 (Peter Nowak)

Case law (General Court)

Case T-51/89 Tetra Pak Rausing SA v Commission of the European Communities, 10.7.1990, ECR II-00309 (Tetra Pak)

Case T-504/93 Tiercé Ladbroke SA v Commission of the European Communities, 12.6.1997, ECR II-00923 (Ladbroke)

Case T-229/94 Deutsche Bahn AG v Commission of the European Communities, 21.10.1997, II-01689 (Deutsche Bahn)


Case T-5/97 Industrie des poudres sphériques SA v Commission of the European Communities, 30.11.2000, ECR II-03755 (IPS)

Joined Cases T-125/97 and T-127/97 The Coca-Cola Company and Coca-Cola Enterprises Inc. v Commission of the European Communities, 22.3.2000, ECR II-01733 (Coca-Cola)

Case T-228/97 Irish Sugar plc v Commission of the European Communities, 7.10.1999, ECR II-02969 (Irish Sugar)

Case T-62/98 Volkswagen AG v Commission of the European Communities, 6.7.2000, ECR II-01707 (Volkswagen)


Case T-139/98 Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission of the European Communities, 22.11.2001, II-03413 (AAMS)

Case T-219/99 British Airways plc v Commission of the European Communities, 17.12.2003, ECR II-05917 (British Airways v Commission)

Case T-52/00 Coe Clerici Logistics SpA v Commission of the European Communities, 17.6.2003, ECR II-02123 (Coe Clerici Logistics)

Case T-57/01 Solvay SA v European Commission, 17.9.2009, ECR II-04621 (Solvay)


Case C-12/03 P Commission of the European Communities v Tetra Laval BV, 15.2.2005, ECR I-00987 (Tetra Laval)

Case T-198/03 Bank Austria Creditanstalt AG v Commission of the European Communities, 30.5.2006, ECR II-01429 (Bank Austria)

Case T-259/03 Kalliopi Nikolaou v Commission of the European Communities, 12.9.2007, ECR II-00099 (Kalliopi Nikolaou)

Case C-310/93 BPB Industries plc and British Gypsum Ltd v Commission of the European Communities, 6.4.1995, ECR I-00685 (BPB Industries)

Case T-340/03 France Télécom SA v Commission of the European Communities, ECR II-00107 (France Télécom)

Case T-161/04 Jordana, 12.9.2007, ECR II-00099 (Jordana)

Case T-201/04 Microsoft Corp. v Commission of the European Communities, 17.9.2007, ECR II-03601 (Microsoft v Commission)

Case T-301/04 Clearstream Banking AG and Clearstream International SA v Commission of the European Communities, 9.9.2009, ECR II-03155 (Clearstream)

Case T-151/05 Nederlandse Vakbond Varkenshouders (NVV), Marius Schep and Nederlandse Bond van Handelaren in Vee (NBHV) v Commission of the European Communities, 7.5.2009, ECR II-01219 (NVV)
Case T-321/05 AstraZeneca AB and AstraZeneca plc v European Commission, 1.7.2010, ECR II-02805 (AstraZeneca)

Case T-446/05 P Amann & Söhne GmbH & Co. KG and Cousin Filterie SAS v European Commission, 28.4.2010, ECR II-01255 (Amann & Söhne)


Case T-342/07 Ryanair Holdings plc v European Commission, 6.7.2010, ECR II-03457 (Ryanair v Commission)


Case T-427/08 Confédération européenne des associations d’horlogers-réparateurs (CEAHR) v European Commission, 15.12.2010, ECR II-05865 (CEAHR)


Case T-79/12 Cisco Systems Inc.and Messagenet SpA v European Commission, supported by Microsoft Corp., 11.12.2013, ECLI:EU:T:2013:635 (Cisco Systems)


Court proceedings (General Court)

**Opinions of Advocate General**

Opinion of Mr. Advocate General Jacobs, 28.5.1998, Case *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG*, ECR I-07791 [1998]

Opinion of the Advocate General Campos Sánchez-Bordona, 12.5.2016, Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:339 [2016]

**Decisions (European Commission, DG Comp)**


Case No IV/M.269 – *Shell/Montecatini* [1994], OJ 1994 L 332/48, Merger Procedure (*Shell/Montecatini*)

Case No COMP/M.1672 – *Volvo/Scania*, Merger Procedure, 15/03/2000 (*Volvo/Scania*)

Case No COMP/M.1741 – *MCIWorldCom/Sprint*, L 300/1, Merger Procedure, 28/06/2000 (*MCIWorldCom/Sprint*)


Case COMP/C-3/39.530 – Microsoft (tying), 16.12.2009 (Microsoft (tying))

Case No COMP/38.784 Wanadoo España vs. Telefónica, Merger Procedure, 04/07/2007 (Telefonica)

Case No COMP/M.4523 – Travelport/Worldspan, Merger Procedure, 21/08/2007 (Travelpport/Worldspan)

Case No COMP/M-4726 – Thomson Corporation/Reuters Group, Merger Procedure, 19/02/2008 (Thomson Corporation/Reuters Group)

Case No COMP/M.4731 – Google/DoubleClick, Merger Procedure, 11/03/2008 (Google/DoubleClick)

Case No COMP/M.4854 – TOMTOM/TELE ATLAS, Merger Procedure, 14/05/2008 (TomTom/Tele Atlas)

Case No COMP/M.5727 – MICROSOFT/YAHOO! SEARCH BUSINESS, Merger Procedure, Brussels 18/02/2010 (Microsoft/YSB)


Case No COMP/M.6281 – MICROSOFT/SKYPE, Merger Procedure, Brussels 07/10/2011 (Microsoft/Skype)


Case No COMP/M.6314 – Telefónica UK/Vodafone UK/Everything Everywhere/JV, 04/09/2012 (Everything Everywhere)

Case No COMP/M.7023 – PUBLICIS/OMNICOM, Merger Procedure, Brussels 09/01/2014 (Publicis/Omnicom)
Case No COMP/M.7217 – FACEBOOK/WHATSAPP, Merger Procedure, Brussels 03/10/2014 (Facebook/WhatsApp I)

Case No COMP/M.7337 – IMS HEALTH/CEGEDIM BUSINESS, Merger Procedure, 19/12/2014 (IMS Health)

Case M.7813 – SANOFI / GOOGLE / DMI JV, Merger Procedure, 23/02/2016 (Sanofi/Google)

Case M.8124 – Microsoft / LinkedIn, Merger Procedure, Brussels 6.12.2016 (Microsoft/LinkedIn)

Case M.8228 – FACEBOOK/WHATSAPP, Merger Procedure, Brussels 17.05.2017 (Facebook/WhatsApp II)

Case AT.39740 Google Search (Shopping), Antitrust Procedure, 27/06/2017 (Google Search (Shopping))

Case AT.40.411 – Google Search (AdSense), Antitrust Procedure, pending (Google AdSense)

Case AT.40.099 – Google Android, Antitrust Procedure, pending (Google Android)

Decisions of the French Competition Authority (L’Autorité de la Concurrence)


Decisions of the Belgian Competition Authority (L’Autorité belge de la concurrence)

Decisions of the Italian Competition Authority (AGCM)


The Federal Court of Justice of Germany (Bundesgerichtshof, BGH)


The Federal Constitutional Court of Germany (Bundesverfassungsgericht, BVerfG)


The District Court of Berlin (Landsgericht Berlin)


The Supreme Court of the United States

United States v. Terminal R.R. Ass’n of St. Louis, 224 U.S. 383, 409 (1912) (Terminal Railroads)

Dictionaries


Primary Legislation


European Convention on Human Rights (EHRC)

Secondary legislation


Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981
Press Releases


Other Official Sources


European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the

European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single market Opportunities and Challenges for Europe, SWD(2016) 172 final (EC Online Platform Communication 2016)

European Commission: Communication from the Commission — Guidance on the Commission’s enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, EUVL C 45, 24.2.2009, s. 7-20 (Guidance on Article 102 TFEU Enforcement Priorities)

European Commission: Communication from the Commission — Notice — Guidelines on the application of Article 81(3) of the Treaty (Text with EEA relevance), EUVL C 101, 27.4.2004, s. 97-118 (EC Guidelines on the application of Article 101(3) TFEU)


Commission of the European Communities: Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information Society, COM(90) 314 final – SYN 297 and 288, Brussels, 13 September 1990 (EC Communication on protection of personal data 1990)


(Autorité de la concurrence & Bundeskartellamt 2016)


European Commission: Article 29 Data Protection Working party, 0829/14/EN WP216 Opinion 05/2014 on Anonymization Techniques, 10.4.2014, WP 216 (EC Opinion on Anonymization Techniques 2014)


European Data Protection Supervisor: Preliminary Opinion – Privacy and competitiveness in the age of big data: The Interplay between data protection,
competition law and consumer protection in the Digital Economy, March 2014 (EDPS Opinion 2014)


EC Consultation on Merger Control Procedural and Jurisdictional Aspects, Non-Confidential Version, 31.1.2017, Microsoft Response (EC Consultation 2017 Microsoft Response)


Speeches


Newspapers / News websites


Web material


EU Focus: Commission fines Google EUR 2.42 billion for giving illegal advantage to own comparison shopping service, EU Focus 2017, 358, p. 3-5 (EU Focus 358/2017)
