IS THE ESSENTIAL FACILITIES DOCTRINE FIT FOR ACCESS TO DATA CASES? THE DATA PROTECTION ASPECT

Rok Dacar*

Abstract: Personal data can be of great economic value for companies as it is an essential input for the offering of a wide array of services. One way for a company to obtain access to essential personal data controlled by another company is by demanding mandatory access on the grounds of the essential facilities doctrine. Such access, however, can violate the right to the protection of personal data of the data subjects if it is not based on one of the legitimate grounds for the processing of personal data set by the GDPR. Two of these grounds are especially likely to be applicable to the access to personal data mandated using the essential facilities doctrine: the interpretation of the Commission decision or the judgment of the Court of Justice ordering the granting of access as a legal obligation and the legitimate interest of the company requesting access, for such access. The anonymisation of personal data is not a viable option for the circumvention of the rules of the GDPR as anonymised personal data loses most of its economic relevance for companies.

Keywords: essential facilities doctrine, right to protection of personal data, grounds for processing personal data, anonymisation of personal data, General Data Protection Regulation.

1 Introduction

Access to competitively relevant data is crucial for companies to compete successfully on today's markets. The importance of such data goes far beyond the ICT sector as data is becoming one of the most important inputs even in traditional, so-called bricks and mortar, sectors (eg mobility, construction, banking, etc). However, one must not overlook that a company's access to personal data controlled by another company might not only increase its competitive potential but also cause widespread violations of fundamental rights of the individuals that the data refers to (data subjects). One of the means for a company to obtain competitively relevant data is by use of one of the most controversial instruments of competition law, the essential facilities doctrine. This paper will explore the possible clash between the obligation of a company to grant access

* Teaching assistant and doctoral student at the Faculty of Law, University of Maribor; mag. iur. (Ljubljana), MA (Bruges). Email: rok.dacar@um.si (ORCID: 0000-0001-8936-9311). DOI: 10.3935/cyelp.18.2022.483.

to the essential personal data it controls and its obligation not to violate the right to the protection of personal data of the data subjects. All this with the aim of answering the research question *whether the current data protection regime in the EU allows for personal data to be shared as essential facilities under the essential facilities doctrine and, if so, under what conditions*.

The paper is divided into four main parts. The first clarifies the basic concepts and institutes necessary for understanding data protection concerns related to the (mandatory) sharing of personal data. It analyses (i) the genesis, nature, and current status of the (fundamental) right to protection of personal data while taking special note of its double-faceted nature; (ii) the genesis of the essential facilities doctrine and the possibility of data being an essential facility; (iii) the difference between personal and non-personal data and some of the difficulties connected with the distinction of the two categories of data; and lastly (iv) the relationship between competition law and data protection. In the second part, the paper analyses under what grounds for the processing of personal data as stated by the General Data Protection Regulation (hereinafter: GDPR)[1] could personal data be shared under the essential facilities doctrine without such sharing constituting a violation of the data protection regime. It is concluded that it could be possible for personal data to be shared under the essential facilities doctrine on two grounds: (i) either a Commission decision or Court[2] judgment ordering the mandatory sharing of personal data which could be interpreted as a legal obligation; or (ii) the company requesting access to personal data could prove it has a legitimate interest to access that data which outweighs the interest of the data subjects for the protection of their personal data. The third part of the paper explores the possibility of personal data being transformed into non-personal data and shared as such. As the rules of the GDPR only apply to personal data, its effective transformation into non-personal data means that the data protection rules no longer apply. There are, however, two limits to such circumvention of the GDPR. Firstly, there is always the possibility of non-personal data being transformed back into personal data through the use of advanced analytics. Secondly, the anonymisation of personal data voids them of most of their commercial value. The fourth and last part of the paper summarises the findings of this study and attempts to present a holistic answer to the research question above.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (hereinafter: GDPR).

[2] The term Court is used to describe both the Court of Justice of the European Union as well as the General Court of the European Union.

2 Setting the scene

2.1 The right to protection of personal data

'The right to protection of personal data is a young fundamental right that in a very short time became one of the core values of EU law'.[3] It is enshrined in Article 8 of the Charter of Fundamental Rights of the EU (hereinafter: the Charter)[4] as well as in Article 16(1) of the Treaty on the Functioning of the EU.[5] The right to protection of personal data is operationalised by the GDPR,[6] a successor of Directive 95/46,[7] introducing detailed provisions on the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[8] The right to protection of personal data was created through the case law of the European Court of Human Rights (hereinafter: ECtHR), where it was first considered only as an informational dimension of the right to respect of personal and family life but later gained the nature of an independent fundamental right, protected through the provisions of Article 8 of the European Convention on Human Rights (right to respect for private and family life),[9] while still being tightly connected with the right to respect of personal and family life. From the ECtHR's case law, it was transplanted into EU law, being recognised as a fundamental right in the Court's *Promusicae*[10] judgment in 2008 and given the nature of an independent fundamental right in the Charter. The close connection between the right to protection of personal data and the right to private and family life is clearly visible from the Court's judgments regarding the right to protection of personal data as they take into

---

[3] Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection' (2016) 23(5) Maastricht Journal of European and Comparative Law 812, 813.

[4] Art 8 of the Charter states that:

'1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority'.

[5] Stating that everyone has the right to the protection of personal data concerning them.

[6] The GDPR confirms that the right to protection of personal data is a fundamental right. Recital 1 states that: 'The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her'.

[7] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.

[8] The GDPR, Art 1.

[9] Gloria González Fuster, *The Emergence of Personal Data as a Fundamental Right of the EU* (Springer 2014) 214.

[10] Case C-275/06 *Productores de Música España (Promusicae)* ECLI:EU:C:2008:54.

consideration the provisions of both Article 7 (respect for private and family life) and Article 8 (right to protection of personal data) of the Charter, which is clearly visible in the *Scheke and Eifert*,[11] *Schwarz*,[12] and *Digital Rights Ireland*[13] cases. The specificity of the right to protection of personal data is that it has a double-faceted character: it is a fundamental right while it also pursues goals of an economic nature.[14]

2.2 The essential facilities doctrine

According to the essential facilities doctrine, the owner of a facility which is not replicable by the ordinary process of innovation and investment, and without access to which competition on a market is impossible or seriously impeded, has to share it with a rival.[15,16] Essential facility

[11] Joined Cases C-92/08 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662 state in para 64 that: 'the publication of data by name relating to the beneficiaries concerned and the precise amounts received by them from the EAGF and the EAFRD constitutes an interference, as regards those beneficiaries, *with the rights recognised by Articles 7 and 8 of the Charter*' (emphasis added).

[12] Case C-291/12 *Schwarz v Stadt Bochum* ECLI:EU:C:2013:670, paras 33, 39, 46, etc.

[13] Case C-293/12 *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238, paras 38–72.

[14] Case C-518/07 *Commission v Federal Republic of Germany* ECLI:EU:C:2010:125 states in para 30 that 'the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a *fair balance between the protection of the right to private life and the free movement of personal data*' (emphasis added); while Case C-582/14 *Patrick Breyer v Federal Republic of Germany* ECLI:EU:C:2016:779 states in para 58 that: 'Article 5 of Directive 95/46 authorises Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful, the margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by that directive of maintaining a *balance between the free movement of personal data and the protection of private life*' (emphasis added); furthermore, recital 2 of the GDPR inter alia states that: 'This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an *economic union, to economic and social progress*, to the strengthening and the *convergence of the economies within the internal market*, and to the well-being of natural persons' (emphasis added); the GDPR also states in Art 1(3) that: 'The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'.

[15] Grainne de Burca and Paul Craig, *EU Law* (6th edn, OUP 2015) 1074.

[16] For a more in-depth analysis of the essential facilities doctrine, see Sebastien J Evrard, 'Essential Facilities, Bronner and Beyond' (2004) 10(3) Columbia Journal of European Law 491; Marina Lao, 'Networks, Access and "Essential Facilities": From Terminal Railroad to Microsoft' (2009) 62(2) SMU Law Review 557; Marina Lao, 'Search, Essential Facilities, and the Antitrust Duty to Deal' (2013) 11(5) Northwestern Journal of Technology and Intellectual Property 275; Devdatta Malshe, 'Essential Facilities: de facto; de jure' (2019) 40(3) European Competition Law Review 124; Axel Beckmerhagen, *Die essential facilities doctrine im US-amerikanischen und europäischen Kartellrecht* (Nomos 2002); Ulf Muller and Anselm Rodenhausen, 'The Rise and Fall of the Essential Facility Doctrine' (2008) 29(5) European Competition Law Review 310.

cases are special types of refusal to sell/refusal to deal cases in which two relevant markets have to be defined: the upstream market and the downstream market. For the essential facilities doctrine to be used, a company with a dominant position on the upstream market must refuse to grant access to a product or service from this market that is necessary to compete on the downstream market (it is an essential facility or essential input) to a company requesting it. The essential facilities doctrine was first conceived by the United States Supreme Court in the famous *Terminal Railroad Combination* case of 1912. The doctrine was developed further by both the Supreme Court and lower, especially federal, courts. In the 1960s and 1970s, it came under heavy fire from anti-interventionist schools of economic and legal thought, one of the most famous critiques being Philip Areeda's article 'Essential Facilities: An Epithet in Need of Limiting Principles'. The Supreme Court's judgment in the *Trinko*[17] case in 2004, with justice Scalia stating that the Supreme Court has never recognised such a doctrine, and thus finds no need either to recognise it or to repudiate it, was the final nail in the coffin for the doctrine in the United States legal system, limiting its use to such an extent as to make it obsolete.

In the EU, however, due to the strong presence of German ordoliberal economic though, the essential facilities doctrine received far less criticism and was widely used by the European Commission and the Court, especially from the 1980s to the early 2000s. The Commission and the Court applied the essential facilities doctrine in a large number of cases concerning, inter alia, chemicals needed to produce other chemicals (*Commercial Solvents*),[18] port infrastructure (*B&I/Sealink*,[19] *Port of Rødby*),[20] services needed for the functioning of airports (*Flughafen Frankfurt/Main AG*,[21] *Alpha Flight Services/Aéroports de Paris*),[22] railroads, trains and train staff (*Night Services*),[23] as well as intellectual property rights (*Volvo v*

[17] Verizon Commc'ns, Inc v Law Offices of Curtis V Trinko, LLP, 540 US 398, 410-411 (2004).

[18] Case C-6/73 *Istituto Chemioterapico Italiano and Commercial Solvents v Commission* ECLI:EU:C:1974:18.

[19] *B&I/Sealink* (Case IV/34.689) Commission Decision 94/19/EC [1994] OJ L15/8.

[20] *Port of Rødby* Commission Decision 94/119/EC [1993] OJ L55/52.

[21] *Flughafen Frankfurt/Main AG* (Case IV/34.801) Commission Decision 98/190/EC [1998] OJ L72/30.

[22] *Alpha Flight Services/Aéroports de Paris* (Case IV/35.613) Commission Decision 98/513/EC [1998] OJ L230/10.

[23] Case T-374/94 *European Night Services Ltd v Commission* ECLI:EU:T:1998:198.

Veng,[24] *Renault v Maxicar*,[25] *Magill*,[26] *IMS Health*,[27] *Microsoft*).[28]

After the heavily criticised[29] *Microsoft* judgment that caused considerable uncertainty about the conditions in which the essential facilities doctrine can be used, both the Commission and the Court showed great reticence towards its application. It is not surprising, then, that the Commission avoided voicing its opinion about the possibility of data being an essential facility despite having several chances to do so, namely in the *Facebook/WhatsApp*,[30] *Google/DoubleClick*,[31] *Telefónica UK/Vodafone UK/Everything Everywhere/JV*[32] cases. Rather than taking a clear stance on the matter, the Commission pointed out that even if one company controls a certain dataset, there is still a large pool of data available for other companies to use and that the use of a certain dataset by one company does not restrain other companies from using this same dataset, as the nature of data is non-rivalrous.[33] While this is true, there can also be cases in which data that another company needs access to, to compete on the downstream market, is in the exclusive control of another company and consequently constitutes an essential facility. Notable examples of such cases are the (i) *GDF Suez*[34] case from France and the (ii) *hiQ Labs*[35] and (iii) *PeopleBrowsr*[36] cases from the USA.

(i) GDF Suez (now Engie) is a French vertically integrated energy company that had a legal monopoly on the distribution of electricity and gas before liberalisation of the sector. The monopoly enabled GDF Suez to create a database containing personal data of its customers. Direct Energie, a competitor of GDF Suez, demanded access to some of the personal data (names, addresses, information about the consumption of gas and phone numbers) included in the database. The French Competition Protection Authority (Authorité de la concurrence) ordered GDF Suez to share the requested data with Direct Energie and to send a letter to the

[24] Case C-238/87 *AB Volvo v Erik Veng* (UK) ECLI:EU:C:1988:477.

[25] Case C-38/98 *Régie nationale des usines Renault SA v Maxicar SpA and Orazio Formento* ECLI:EU:C:2000:225.

[26] Case C-241/91 P, C-242/91 P *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission* ECLI:EU:C:1995:98.

[27] Case C-418/01 *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* ECLI:EU:C:2004:257.

[28] Case T-201/04 *Microsoft v Commission* ECLI:EU:T:2007:289.

[29] One of the most pertinent critiques being Renata B Hesse, 'Counselling Clients on Refusal to Supply Issues in the Wake of the EC Microsoft Case' (2008) 22(2) Antitrust 32.

[30] *Facebook/WhatsApp* (Case COMP/M.7217) (2014).

[31] *Google/DoubleClick* (Case COMP/M.4731) [2008] OJ C184/9.

[32] *Telefónica UK/Vodafone UK/ Everything Everywhere/ JV* (Case COMP/M.6314) (2012).

[33] Bruno Lasserre and Andreas Mundt 'Competition Law and Big Data: The Enforcers' View' (2017) 1(4) Rivista Italiana di Antitrust 87, 97.

[34] Decision of the Authorité de la concurrence GDF Suez 14-MC-02, Judgment of the Appellate Court no 2014/19335 and of the Cassation Court no 31 F-D.

[35] *hiQ Labs, Inc v LinkedIn Corp*, 938 F.3d 985 (9th Cir 2019).

[36] *PeopleBrowsr, Inc v Twitter, Inc*, Case No. 3:12-cv-06120-EMC.

customers whose personal data was about to be shared, informing them that they can deny the consent for their data to be shared by filling out a special form and sending it to GDF Suez. Should they not send such a letter, consent would be presumed. It is important to note that the decision was passed before the coming into force of the GDPR, according to which 'silence, pre-ticked boxes or inactivity should not constitute consent'.

(ii) HiQ Labs was using publicly available LinkedIn data to prepare a statistical analysis of different workforce trends. LinkedIn prohibited hiQ Labs from further using its data, thereby refusing them access to an essential input. After an appeal to the Supreme Court, the case was referred back to the Ninth Circuit Court.

(iii) PeopleBrowsr was using publicly available Twitter data to analyse the attitude of users towards different products and influencers. Similar to the *hiQ Labs* case, Twitter barred PeopleBrowsr from using the essential data. The case was resolved with a settlement granting PeopleBrowsr access to Twitter data for an additional limited amount of time.

Furthermore, the tenth amendment to the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen)[37] introduced the provision of Article 19(4) explicitly stating that data can be an essential facility.[38] We can therefore conclude that despite the fact that neither the Commission nor the Court has considered data as an essential facility up to this point, data can still be an essential facility. The exact conditions that must be fulfilled for data to be an essential facility will not be further analysed as this is not the aim of this paper. Its aim is rather to clarify under what conditions obligatory sharing of personal information does not infringe the right to the protection of personal information.

Data, and especially big data, has several characteristics that distinguish it from traditional materialised and immaterialised (essential) facilities: its decreasing marginal value,[39] decreasing value over time,[40] in some cases its non-rivalrous nature,[41] and the extreme network effects

[37] Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S.1750, 3245), das zuletzt durch Artikel 4 des Gesetzes vom 20. Mai 2022 (BGBl. I S. 730) geändert worden ist (2013 Act against Restraints of Competition (FRG)).

[38] The provision states that: 'An abuse exists in particular if a dominant undertaking as a supplier or purchaser of a certain type of goods or commercial services refuses to supply another undertaking with such a good or commercial service for adequate consideration, in particular to grant it access to data, networks or other infrastructure facilities, and if the supply or the granting of access is objectively necessary in order to operate on an upstream or downstream market'.

[39] The more data a company controls the smaller is the economic value of any additional quantity of data.

[40] Data is especially relevant when 'fresh'. The more time that passes from the collection of data, the smaller is its economic value due to market changes.

[41] In general, the use of a certain dataset by one company does not exclude other companies from using the same dataset as well.

present in data-related industries.[42] Taking account of these specificities, two distinct schools regarding the possible nature of data as an essential facility have developed. The first argues that data can never be an essential facility[43] while the second defends the position that data can and even should be an essential facility if certain conditions are met, as a refusal to grand access to data can have the same effects for competition on a downstream market as refusal to grand access to a traditional facility.[44] One could argue that the uncertainties in academia regarding the possible nature of data as an essential facility ended with the tenth amendment of the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen)[45] that recognises the possible nature of data as an essential facility.[46]

Access to relevant data can be of vital importance for companies, as it is impossible to offer some services without relevant data (data is an essential input). Given that the vast majority of economically relevant data is controlled by a handful of large companies, the so-called FAANG (Facebook (now META), Amazon, Apple, Netflix and Google (now Alphabet)) companies and some other international corporations, it can be difficult for smaller companies to obtain relevant data, especially due to the prohibitively large investments needed for setting up an efficient data collection and analysis operation. Currently, access to only very limited categories of data, for example auto-diagnostics[47] and some electricity consumption data,[48] is subject to ex ante regulation in the EU. Conse-

---

[42] See *Google Search (Shopping)* (Case AT.40099) Commission Decision AT.39740 [2018] OJ C9, para 287, 319.

[43] Erika Douglas, 'Monopolization Remedies and Data Privacy' (2020) 24(1) Virginia Journal of Law and Technology 1; Zachary Abrahamson, 'Essential Data' (2014) 124(3) Yale Law Journal 867.

[44] Édouard Bruc, 'Data as an Essential Facility in European Law: How to Define the "Target" Market and Divert the Data Pipeline' (2019) 15(2/3) European Competition Journal 177.

[45] 2013 Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen) (FRG).

[46] Art 18/III/3 states that '(3) In assessing the market position of an undertaking in relation to its competitors, account shall be taken in particular of the following … its access to data relevant for competition'. Art 19/II/4 states that '(2) An abuse exists in particular if a dominant undertaking as a supplier or purchaser of a certain type of goods or commercial services. … 4. refuses to supply another undertaking with such a good or commercial service for adequate consideration, in particular to grant it access to data, networks or other infrastructure facilities, and if the supply or the granting of access is objectively necessary in order to operate on an upstream or downstream market and the refusal threatens to eliminate effective competition on that market, unless there is an objective justification for the refusal'.

[47] Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles [2007] OJ L 263.

[48] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) [2019] OJ L158.

quently, the only available tool for gaining access to the vast majority of economically relevant data that the company controlling it does not want to share is the use of the doctrine. This might, however, change with the adoption of the proposed Digital Markets Act (DMA) which, inter alia, states that gatekeepers are to 'provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services …',[49] as well as the proposed Data Act.[50,51]

2.3 The relation between competition law and data protection law

The relation between competition law and data protection law is largely shaped by the Court's *Asnef-Equifax*[52] judgment in which it stated that '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'.[53] The Commission followed this position in the *Facebook/WhatsApp* and *Google/DoubleClick* merger decisions in which it, inter alia, stated that 'any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules'.[54] Despite some authors arguing that the Court has taken a clear position that questions related to the protection of personal data are not relevant for competition law under any circumstances,[55] its position is in fact much more moderate than might seem on first sight. The phrase '*as such*' used by the Court in the *Asnef-Equifax* judgment means that questions related to the protection of personal information are not relevant in competition law assessments only if they apply solely to the protection of personal information. As soon as the protection of personal information has any impact on competition law or market competition, it can, consequently, be considered in competition law assessments. Such an interpretation of the *Asnef-Equifax* judgment is in line with the institution's position in some other cases where it used competition law

[49] Proposal for a regulation of the European parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final, Art 6(i).

[50] Proposal for a regulation of the European parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.

[51] For a more detailed analysis of the Data Act proposal, see Clément Perarnaud and Rosanna Fann, 'The EU Data Act: Towards a New European Data Revolution?' (*CEPS*, 4 March 2022) <https://www.ceps.eu/download/ publication/?id=35693&pdf=CEPS-PI2022-05_The-EU-Data-Act.pdf> accessed 10 September 2022.

[52] Case C-238/05 *Asnef-Equifax* ECLI:EU:C:2006:734.

[53] ibid, para 63.

[54] *Google/DoubleClick*, para 164.

[55] Charlotte Breuvart, Éthienne Chassing and Anne-Sophie Perraut, 'Big Data and Competition Law in the Digital Sector: Lessons from the European Commission's Merger Control Practice and Recent National Initiatives' (2016) no 3, Concurrences – revue des droits de la concurrence, 51.

instruments to address certain goals that were not directly connected with market efficiency or even impacted it negatively.[56] An example is the Commission's *EMI/Universal*[57] merger decision that required Universal to make strict commitments meant to prevent the endangerment of cultural diversity protected through Article 167 TFEU. Given the Court's position regarding the relation between competition law and data protection, there is no hindrance to take data protection considerations into account when using the doctrine to mandate obligatory access to personal data, all the more so as the protection of personal information is a fundamental right.

A position favouring a much closer connection between competition law and data protection law was taken by the German Competition Authority (Bundeskartellamt (BKA)) in its recent decision in the *Facebook* case.[58] According to the BKA, Facebook abused its dominant position on the market for social networks by forcing its users to accept terms of service that infringed their right to the protection of personal information and their right to informational self-determination, as they had to comply with those terms (and thus allowing Facebook to collect a large amount of data produced by them online, even when not using Facebook) if they wished to use Facebook's services, for which there were no actual or potential substitutes available. The decision was later overturned by the national judiciary and the case was referred to the Court for a preliminary ruling. In the author's opinion, the Court will not stray from the position established in its *Asnef-Equifax* judgment and will thus not follow the revolutionary reasoning of the BKA.[59]

2.4 The distinction between personal and non-personal data

As possible violations of the right to the protection of personal data can only arise from the misuse of personal data, we must distinguish between personal and non-personal data. The GDPR defines personal data as

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[60]

---

[56] Maria Wasastjerna, *Competition, Data and Privacy in the Digital Economy: Towards a Privacy Dimension in Competition Policy?* (Wolters Kluwer 2020) 57.

[57] *Universal Music Group/EMI Music* (Case COMP/M.6458) (2012).

[58] Bundeskartellamt case no B6-22/16.

[59] For more on the Facebook case, see Klaus Wiedemann, 'A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v Facebook (Case KVR 69/19)' (2020) 51(9) International Intellectual Property and Competition Law 1168; Anne Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021) 66(2) Antitrust Bulletin 276.

[60] GDPR, Art 4(1).

If such data is processed wholly or partly by automated means, the rules of the GDPR apply, with the term 'processing' also covering the disclosure by transmission of personal data from one company to another.[61] As sharing of personal data mandated by the essential facilities doctrine represents disclosure by transmission, it constitutes processing of personal data and must be in accordance with the provisions of the GDPR.

The definition of non-personal data is a negative one, meaning that all data that does not meet the requirements of the above definition is non-personal data. However, the line between personal and non-personal data is not always clear cut and the distinction between the two categories of data is therefore artificial to a certain extent. This is especially true as the constant technological advances in data analytics can lead to the combination and analysis of two different datasets containing non-personal data to produce personal data.[62] The Court has developed a wide body of case law regarding the distinction between personal and non-personal data. In the *Breyer*[63] case, the question arose about whether a log of accesses to the websites of the German government, containing the IP addresses of the computers from which the websites were visited, constituted personal data. While the log did contain the IP addresses, it was not possible to identify the individuals who visited the websites without the assistance of the Web Service Provider which was able to link the IP addresses to individuals.[64] The Court noted that 'the fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46,'[65] thereby confirming that the data in question indeed constituted personal data. Some time later in the *Nowak*[66] case, the Court concluded that the handwritten exam sheets by an examination candidate may constitute personal data. The *Nowak* case importantly confirmed that the use of the expression 'any information' in the definition of the concept of 'personal data', in Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective

[61] Art 4(2) GDPR states that 'processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

[62] Thomas Tombal, 'Economic Dependence and Data Access' (2020) 51(1) International Review of Intellectual Property and Competition Law 70, 90.

[63] Case C-582/14 *Breyer v Federal Republic of Germany* ECLI:EU:C:2016:779.

[64] Cristopher Docksey and Hielke Hijmans, 'The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' (2019) 5(3) European Data Protection Law Review 300, 302–303.

[65] Case C-582/14 *Breyer v Federal Republic of Germany* ECLI:EU:C:2016:779, para 44.

[66] Case C-434/16 *Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994.

but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.[67] The two cases lead us to conclude that the Court promotes a wide interpretation of personal data, as personal data does not have to be sensitive in nature, nor does it need to be directly linked to a data subject.

A dataset to which access is requested using the doctrine can contain personal data, non-personal data or a mix of both. If it contains only non-personal data, the data protection regime does not apply. However, as soon as the dataset in question contains some personal data which is wholly or partly processed by automated means, the requirements of the GDPR must be taken in account. This means that access to a dataset containing only non-personal data could be mandated through the doctrine by using the conditions applicable to non-materialised facilities,[68] without the need for compliance with the GDPR, while access to a dataset containing any amount of personal data would have to comply with the GDPR. It is foreseeable that the majority of data access claims will be centred on datasets containing at least some personal data, both because the term personal data is interpreted broadly and because personal data is usually commercially far more valuable than non-personal data, since it is an essential input for targeted advertising, whereas the commercial value of non-personal data is much lower.[69] Besides, in the future personal data will be necessary to offer services connected to innovative sectors such as smart mobility, smart living, etc, which will further increase the demand for such data.

3 Possible grounds for obligatory sharing of personal data

Obligatory sharing of essential personal data mandated through the use of the essential facilities doctrine would have to meet at least one of the criteria for the lawfulness of processing of personal data as laid down by the GDPR in Article 6.[70] In the following section, the paper analyses

[67] ibid, para 34.

[68] The Court still has to clarify if these are the *IMS Health* or the *Microsoft* criteria.

[69] In all the three above-mentioned data access cases (*GDF Suez*, *PeopleBrowsr* and *HiQ Labs*) the required data was personal data.

[70] Art 6(1) GDPR states that:
'Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks'.

how likely it would be for such data sharing to fulfil one of those conditions.

– The condition that the data subject has given consent to the processing of his or her personal data for one or more specific purposes can realistically not be fulfilled in connection with the essential facilities doctrine as it means that the company that would be ordered to share the personal data it controls would have to obtain the consent of each of the data subjects whose personal data the dataset it shares contains. Most competitively relevant datasets contain personal data from a great number of data subjects (from several tens of thousands upwards, even several hundred million). For the condition to be met, each of those data subjects would have to consent to the whole dataset being shared as it would most likely be impossible to separate the data from the data subjects that consented to their personal data being shared from the data of those who did not. The consent would have to have an active, affirmative form as the GDPR explicitly states that inactivity or silence does not constitute consent.[71] Furthermore, when the data is shared, the company obtaining it would have to acquire consent in the above-mentioned form from the data subjects for each individual operation of data processing. In practice, this would mean that the data would be useless as it would be impossible to process it without violating the rules of the GDPR.

– The condition that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract is met when the data subject and the data processor enter into a contractual relationship that can only be fulfilled if the data subject's personal data is processed by the data processor. An example would be the data processor's offering of certain services that require the data subject's data to be processed (for example, remote health diagnostics). As this condition applies only to purely contractual relationships governed by the law of obligations, it is not foreseeable that it would be relevant for the sharing of personal data mandated through the essential facilities doctrine.

– The processing of personal data is legal if it is done to protect the vital interests of the data subject or of another natural person. As the essential facilities doctrine is a tool to enable the company requiring access to an essential facility to compete on the downstream market and not to protect the interests of any kind of individual persons, this condition cannot be met.

---

[71] Recital 32 of the GDPR states that: 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes, or inactivity should not therefore constitute consent'.

– It is highly unlikely that the obligatory sharing of personal data mandated through the essential facilities doctrine would be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This condition can only be applied to public bodies and private bodies vested with the powers of public authorities. In the existing case law of the Commission and of the Court, there has not been a single company that has demanded access to an essential input through the essential facilities doctrine that was vested with such powers. Therefore, while it remains theoretically possible that a private body vested with the powers of public authority would need essential data to carry out tasks in the public interest on the downstream market, such a situation is highly unlikely as it is very difficult to imagine a task carried out in the public interest on a downstream market that would require access to essential personal data.

– A likely legal base for the obligatory sharing of personal data mandated through the use of the essential facilities doctrine would be the requirement that the processing is necessary for compliance with a legal obligation to which the controller is subject. A Commission decision and a Court judgment mandating access to essential data could constitute a sufficient legal base for the processing (sharing) of personal data. According to the GDPR, a legal base does not have to be a legislative act or a general and abstract legal act but can also be an individual and concrete legal act, as long as it is clear, precise and its application foreseeable to the subject it applies to.[72] The Commission is empowered to take actions in cases of abuses of dominant positions by Regulation 1/2003[73] which could also be interpreted as a legal obligation[74] as laid down in the GDPR.

– Processing of personal data is not in violation of the GDPR if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

[72] Recital 41 of the GDPR states that: 'Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the "Court of Justice") and the European Court of Human Rights'.

[73] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002] OJ L1.

[74] Art 7(1) of Regulation 1/2003 states that: 'where the Commission, acting on a complaint or on its own initiative, finds that there is an infringement of Article 81 or of Article 82 of the Treaty, it may by decision require the undertakings and associations of undertakings concerned to bring such infringement to an end. For this purpose, it may impose on them any behavioural or structural remedies which are proportionate to the infringement committed and necessary to bring the infringement effectively to an end. Structural remedies can only be imposed either where there is no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the undertaking concerned than the structural remedy. If the Commission has a legitimate interest in doing so, it may also find that an infringement has been committed in the past'.

which require protection of personal data, in particular where the data subject is a child. Of all the legal bases for the processing of personal data, this one is the broadest and we can well imagine that it could also cover obligatory data sharing mandated through the essential facilities doctrine. The phrase 'legitimate interest' is not defined in the GDPR (as it includes only illustrative examples) so it is possible that the commercial interests of a company to gain access to essential data necessary for competing on the downstream market might constitute a legitimate interest.[75,76] Once a legitimate interest of a company (a third party, as it is illogical for the controller to have any (legitimate) interest in the mandatory sharing of the personal data it controls since such sharing weakens its position on the market) is established, it is necessary to weigh it against the interests and reasonable expectations of the data subjects for the protection of their personal data.[77] This means that in cases where the data subjects reasonably expect their personal data not to be processed by the controller (shared by the company that controls it) or where the personal data contains highly sensitive information (eg about sexual orientation, home address, political affiliation, etc), the legitimate interest of the company requesting access to personal data would probably not override the interests of the data subjects for the protection of their personal data. However, if the data subjects were to reasonably expect that their personal data might be further processed (shared) or if the personal data contained non-sensitive personal information (eg about the consumption of electricity or gas), the commercial interests of the company requesting access to the personal data might outweigh the interests of the data subjects. Such weighing of interests is, of course, problematical, as it is difficult to establish how sensitive personal data is, especially due to the fact that it is possible to combine several datasets consisting of non-sensitive or even non-personal data to obtain highly sensitive personal data. To sum up, in the analysis of whether the interests of a company to gain access to competitively relevant personal data through the use of the essential facilities doctrine outweigh the interests of the data subjects for the protection of their personal data, a three-part test has to be made. 'Firstly, a legitimate interest of the company requesting access to the personal data must be established, secondly, the processing of personal data

[75] The UK Information Commissioner's Office <https://ico.org.uk/for-organisations/guide-to-data-protection/ guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 30 April 2022 states that: 'The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests, or broader societal benefits'.

[76] Recital 47 of the GDPR states that: 'Legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller'.

[77] In recital 47, the GDPR further states that: 'The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing'.

must be essential to achieve it, meaning there are no other, less intrusive possibilities, and thirdly, the interests of the company to gain access to the essential data must be weighed against the interests of the data subjects for their personal data not to be processed'.[78]

4 Anonymisation and pseudonymisation as possible circumventions of the data protection regime?

If the above analysed conditions for the lawfulness of processing personal data are not met, personal data cannot be shared without violating the rules of the GDPR. A possible solution to allow personal data to be shared even beyond the conditions set in Article 6 GDPR is its transformation into non-personal data, that is, anonymisation.[79] Firstly, anonymisation must not be confused with pseudonymisation. Pseudonymisation[80] takes place by replacing an attribute with another attribute, thereby making it more difficult to connect the data with the data subject. Pseudonymised data can still be (indirectly) linked with a data subject with the use of additional data or information, meaning that the data subject is not identified but still identifiable. Therefore, pseudonymised personal data is still personal data and the data protection rules have to be applied, as was confirmed in the *Nowak* judgment.[81] The most common definition of anonymisation[82] on the other hand is that it is the process by which personal data is irreversibly altered in such a way that a

[78] The UK Information Commissioner's Office (n 75).

[79] In recital 26, the GDPR states that: 'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

[80] Defined in Art 4(5) GDPR as: 'the means for the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

[81] Furthermore, in recital 6 the GDPR states that: 'the principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors.'

[82] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 15 April 2022, describes the two main techniques of anonymization as randomization and generalization. Randomization removes the link between the personal data and the data subject by either by changing attributes in the dataset so that they are less accurate while they retain the overall distribution or by shuffling the values of attributes and linking them to different data subjects (permutation). Generalization consists of diluting the attributes of data subjects by modifying the respective scale or order of magnitude (for example instead of the category of people who weigh between 60-65 kilos the category of people who weigh between 55–75 kilos is used).

data subject can no longer be identified directly or indirectly, either by the personal data controller alone or in collaboration with any other party.[83] The definition above is only partially correct, as the perfect anonymity (a type of anonymity where the re-identification of the data subject by the processor or third parties is even theoretically impossible) described by it does not exist, since there is always a slight chance of the identity of the data subject being revealed (a process called re-identification). In particular, the connection of several anonymised datasets and their analysis with advanced analytical methods can lead to the re-identification of the data subject(s), a phenomenon called the mosaic effect.[84] For example, 'credit card transactions, location data from a mobile phone, smartcard tap-in tap-out, and browsing (URLs) datasets have all been shown to be re-identifiable'.[85] This not only happens with the processor or a third party wanting to re-identify one or more data subjects but also by chance when datasets are connected with new datasets that were not considered when anonymising the primary dataset.[86] European data protection law did not adopt the concept of perfect anonymisation, but rather relies on the concept of effective anonymisation, whereby data is considered anonymised when the re-identification of the data subject(s) is unlikely.[87]

An important drawback of the anonymisation of personal data is that it voids personal data of all or of most of its economic relevance. Companies are interested in personal data for the precise reason that they can relate the data to identified individuals, to whom they can, according to their behaviour, their wants and needs, revealed through the analysis of personal data, offer products and services they are most likely to buy. For example, around 98% of the revenues of Meta (Facebook) are gained through the offering of services of targeted advertising. The Facebook app monitors the web pages the user is visiting and adjusts the adverts shown by the Facebook app accordingly. If a user is visiting the web page of a certain car manufacturer, the Facebook app is more likely to show adverts for cars that this particular brand is producing. Meta (Facebook) usually gets paid for each click on the advertisement (pay-per-click) and therefore has an interest to offer highly personalised adverts as users are more likely to click on them than on random adverts. When personal data is anonymised, it is no longer possible for companies to relate the data to identified individuals and therefore such data cannot be used for the

[83] ISO standard 29100, point 2,2 <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en> accessed 19 April 2022.

[84] Timothy Asta, 'Guardians of the galaxy of personal data: assessing the threat of big data and examining potential corporate and governmental solutions' (2017) 45(1) Florida State University Law Review 261, 275.

[85] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era' (2019) 78 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 13 April 2022.

[86] Lilijana Selinšek, 'Veliko podatkovje v pravu in ekonomiji: veliki izzivi ali velike težave?' (2015) 7(2) LeXonomica 161, 177.

[87] Crémer, de Montjoye and Schweitzer (n 85).

same purposes as personal data, but rather only for the identification of the preferences of a certain part of the population (of all the data subjects whose personal data is anonymised), which can also be obtained by financially less burdensome means. It must be noted that anonymisation is also a form of processing of personal information and therefore must fulfil the requirements of the GDPR. Anonymisation is thereby considered to be compatible with the original purposes of the processing only if the anonymisation process is such as to reliably produce anonymised information while the anonymised data must also be retained in an identifiable format to enable the exercise of access rights by data subjects[88] as required by the Court's *Rijkeboer*[89] judgment.[90]

5 Findings

Even though data has until now not been considered an essential facility by the Commission and the Court, there is no obstacle for it to be an essential facility if the company controlling it has a dominant position on the upstream (data) market and refuses to grant a competitor on the downstream market access to the data necessary for competing on this market. A typical situation in which access to data could be demanded on grounds of the doctrine is one where a smaller company would need relevant data to conduct its business activities on the downstream market with that data being under the sole control of a large company on the upstream market, as was the case in the above-mentioned *hiQ Labs* and *PeopleBrowsr* cases. Despite the fact that data has some characteristics that distinguish it from traditional essential facilities (its non-rival nature, omnipresence, etc), a situation can arise in which only one company controls a certain dataset necessary for competing on a connected (downstream) market as was the case in the *GDF Suez* case in France and the *hiQ Labs* and *PeopleBrowsr* cases in the USA. The possibility of data constituting an essential facility was clear and present enough for the German legislator to explicitly state in the last amendment to the Act against Restraints of Competition that data can be an essential facility. As most competitively relevant data is personal data, its mandatory sharing under the essential facilities doctrine not only raises traditional ques-

---

[88] Art 29 Data Protection Working Party 7.

[89] Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M E Rijkeboer* ECLI:EU:C:2009:293.

[90] The judgment stated in para 70 that: 'Article 12(a) of the [95/46] Directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller'.

tions about the determination of a facility as an essential facility[91] but also questions related to the permissibility of sharing the data in regard to the data protection regime in force in the EU. Furthermore, even the mandatory sharing of non-personal data could prove problematic from the data protection perspective as it is possible to extract personal data from non-personal data through the combination of several datasets containing non-personal data and the use of advanced analytics. Personal data was interpreted broadly by the Court, meaning that the GDPR applies when processing a wide array of data, even data that is not by nature sensitive or private.

Processing of personal data is permissible if one or more of the six grounds for the legality of processing personal data laid down in Article 6 GDPR are met. The mandatory sharing of personal data through the essential facilities doctrine is likely to meet two of them: the ground that the processing of personal data is a legal obligation of the processor and the ground that either the controller or the third party has a legitimate interest to process the personal data. Firstly, a Commission decision or Court judgment ordering mandatory sharing of personal data with the essential facilities doctrine could be interpreted as a legal obligation to which the controller is subject. The term legal obligation is interpreted broadly in the GDPR, with it being not only a legislative act but also other kinds of general and abstract or individual and concrete legal acts as long as they are clear, precise and their application is foreseeable to the subject they apply to. Commission decisions and Court judgments are likely to meet these criteria as they must be clear and precise by nature. Furthermore, the application of the essential facilities doctrine to a dataset containing essential personal data is also at the very least foreseeable for the companies controlling such data as the essential facilities doctrine is well established in both the Commission's as well as the Court's case law. Secondly, mandatory sharing of personal data through use of the essential facilities doctrine could also constitute a legitimate interest of a third party, namely the company requesting access, as legitimate interests can also be interpreted as the commercial interests of companies. The legitimate interest of a company to gain access to competitively relevant personal data would have to be weighed against the interests of the data subjects for the protection of their personal data. If the data subjects could not reasonably expect their personal data to be shared with the requesting company or if their interests for the protection of their personal data outweighed the interests of the requesting company to gain access to their personal data, the sharing of such data would not be permissible. If, however, the data subjects were to reasonably expect their personal

[91] Whether it is essential in the sense that the refusal to grand access excludes (all or a considerable amount of) competition from the secondary (downstream) market, there are no actual or potential substitutes for the facility and the refusal does not have an objective justification. In the cases of intellectual property rights (non-materialised facilities), the refusal to grand access to the facility must also preclude the emergence of a new product or at least a technical development of the existing product for which there is consumer demand.

data to be shared with the requesting company or if the interest of the requesting company to gain access to that data outweighed the interests of the data subjects for the protection of their personal data, then such data could be shared through the use of the essential facilities doctrine. In the author's opinion, it would not be easy to weigh the interests of the data subjects against the interests of the requesting company, especially given the double-faceted nature of the right to the protection of personal data which is a fundamental right that also pursues goals of an economic nature. The sharing of personal data could be permissible if the personal data does not contain very intimate information but rather information of a more objective kind (consumption of electricity or gas, etc). However, such classification could prove problematic as even personal data of a non-intimate or non-sensitive character could reveal such intimate or sensitive information if it was subjected to the appropriate analytical process (for example, an analysis of the data on electricity consumption could reveal the marital status of a data subject, her or his daily routines, habits, social status, etc). The ground of legitimate interest is vague and open to (too much) interpretation and therefore the ground of legal obligation constitutes a more appropriate legal basis for mandatory sharing of personal data through the use of the essential facilities doctrine. Furthermore, if a Commission decision or a Court judgment constitutes a legal obligation as stated by the GDPR, the ground of legitimate interest becomes void, as any obligatory data sharing mandated by such a legal act would automatically constitute a sufficient basis for the sharing of personal data and it would thus not be necessary to prove that the requesting company has a legitimate interest to gain access to such data.

Another possibility that would allow for the sharing of personal data mandated through the essential facilities doctrine would be their anonymisation. The GDPR only applies to personal data, meaning that the grounds for the legality of processing of personal data do not apply to non-personal data. In fact, the sharing of non-personal data is currently not regulated by any systematic legal act in the EU, and it is up to the parties of a contract to decide on the arrangements for the sharing of such data. If personal data could be effectively anonymised, it could be shared like any other (traditional) essential facility, without having to take account of the special considerations related to the protection of the right to the protection of personal data. However, the anonymisation of personal data has two main drawbacks that severely limit its effectiveness as a means of circumventing the provisions of the GDPR and enabling the sharing of anonymised personal data. Firstly, there is no perfect anonymisation as it is always possible to re-identify the data subjects by using advanced analytics and combining the non-personal data in question with other non-personal data. This means that there is invariably a realistic possibility that the data subjects will be re-identified, either voluntarily or even non-voluntarily by chance in the process of data analysis. Secondly, personal data is valuable to companies as it enables them to identify the interests of identified or at least identifiable individuals that they

can then use for commercial purposes (eg for targeted advertisements). In other words, personal data is valuable exactly because it is personal data. Were personal data transformed into non-personal data, this would void it of all or in the best case of most of its value for companies, as such data could not be used to identify the preferences of data subjects but merely the average interests of a certain part of the population that could also be identified through financially less burdensome means. This leads us to conclude that anonymisation is not an appropriate tool to enable the sharing of personal data as an essential facility.

6 Conclusion

Having concluded the analysis, we can establish that the most appropriate basis for the sharing of personal data mandated through the essential facilities doctrine is the interpretation of the Commission decision or Court judgment ordering the mandatory sharing of such data as a legal obligation. As any Commission decision or Court judgment would be a legally binding basis for the obligatory sharing of personal data, both institutions (as well as national competition protection agencies and courts) which show great reticence in the use of the doctrine even in cases of more traditional facilities would most probably apply the doctrine in an even more conservative manner in cases where personal data were involved. In the author's opinion, this leaves open the question of whether the doctrine would, in practice, be an effective tool for obtaining competitively relevant personal data. This could prove problematic as it is not possible to systematically mandate access to personal data by using ex ante regulation, since data is not an economic sector but is rather present in all economic sectors, with its specificities varying greatly from one sector to another.

Suggested citation: R Dacar, 'Is the Essential Facilities Doctrine Fit for Access to Data Cases? The Data Protection Aspect' (2022) 18 CYELP 61.