eLaw
Working Paper Series

No 202ť/00# - ELAW– 202ť

\~uoqxq ,pm¡m

c t¦,¡tq,Qa,r¢zpmyqz¡mx,~ust¡,¡{,pm¡m,
|~{¡qo¡u{z,ymwq ,pm¡m,{¤zq~ tu|,¢z ¢ ¡muzmnxq
O¢ ¡q~ ,N:T:Y:,mzp,Ymxsuq~u,S:,

Universiteit Leiden
eLaw

Discover the world at Leiden University

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data

Bart Custers[a,*], *Gianclaudio Malgieri*[b]

[a] *eLaw, Center for Law and Digital Technologies, Leiden University*
[b] *Augmented Law Institute, EDHEC Business School, France*

ARTICLE INFO

Keywords:
Data ownership
Data subject rights
Digital single market
EU charter of fundamental rights
EU data economy
GDPR
Right to data protection
Inalienability for fundamental rights
Personal data
Privacy

ABSTRACT

Many free online services, including search engines and social media, use business models based on the collecting and processing of personal data of its users. The user data are analysed, leased or sold to generate profits. Basically, the users are not paying for the services with subscription fees or any kind of monetary payment, but with their personal data. In this paper, we argue that these business models, treating personal data as a commodity, are problematic under EU data protection law, which disqualifies personal data as a commodity. Both under the EU Charter of Fundamental Rights and the General Data Protection Regulation (GDPR), the legal rights to data protection are inalienable. This is at odds with the actual trade in personal data in the data economy, since the 'payment' cannot be a transfer of ownership of personal data. It could be argued that the 'payment' is not a transfer of ownership of personal data, but rather a transfer of personal data rights, i.e., granting a right to collect and process the data. However, even from that perspective, users would retain inalienable rights to stop or restrict the data processing, as the GDPR does not allow mandating data subject rights to others. Because the legal basis for the processing of personal data is often consent, people can invoke their data subject rights (and thus withdraw their 'payment') at any time and at will after having received (access to) online services. This causes considerable legal uncertainty in transactions, particularly on the side of data controllers, and may not contribute to the EU's envisioned data economy.

1. Introduction

Many free online services, including search engines and social media, use business models based on the collecting and processing of personal data of its users. The user data are analysed, leased or sold to generate profits. Basically, the users are not paying for the services with subscription fees or any kind of monetary payment, but with their personal data. In essence, this means that people do pay for these services, but not with money. Their personal data represents value which is exchanged for these services, sometimes explicitly, but often implicitly, without users knowing which data they actually provide and what the value of their personal data is to these data controllers. Paying with your personal data involves paying with your (informational) privacy.

* Corresponding author.
E-mail address: b.h.m.custers@law.leidenuniv.nl (B. Custers).

https://doi.org/10.1016/j.clsr.2022.105683

From an economic perspective, the way data is currently traded resembles a classic exchange trade economy, which does not involve or require money. Paying for a bread with a chicken does not require any use of money. Such direct payments without any money involved can be used for exchange trade of products (like a bread or a chicken) or services (like cooking a meal or dressing someone's hair) or both, depending on what actors agree upon. However, payment with personal data is fundamentally different from payment with a traditional product or service. The reason for this is that, in the EU, there does not exist data ownership of personal data. This means that people cannot pay with their data, essentially because it is *not theirs to give*.

In a previous article in this journal, we argued that data subjects should perhaps be informed of the economic value that their data represents.[1]. Considering the information asymmetry between data subjects and data controllers, increased awareness about the transactional use and value of personal data might be necessary.[2] Some recent EU legislation implicitly encouraged this approach when recognising the factual reality of personal data used as counter-performance for the provision of digital content or services.[3]

However, this proposal to inform people of the value of their data should not be read as a suggestion or an approval to use personal data as a tradeable commodity.[4] In this paper, we argue that the business models in which people pay with their personal data (and more generally with their privacy) are problematic under EU data protection law. Both under the EU Charter of Fundamental Rights ('the Charter') and the General Data Protection Regulation (GDPR), the legal rights to data protection are inalienable, which essentially prohibits data ownership. Hence, the 'payment' cannot be a transfer of ownership of personal data. It could be argued that the 'payment' is more something like granting a right to collect and process the data.[5] However, even from that perspective, users would retain inalienable rights to stop or restrict the data processing. Because the legal basis for the processing of personal data is often consent, people can invoke their data subject rights (and thus withdraw their 'payment') at any time and at will after having received (access to) online services. This causes considerable legal uncertainty for actors in the data economy.

Just to avoid any misunderstanding, in this paper we do not argue for or against personal data ownership. There is an ongoing debate on this, with solid arguments on both sides. Here, we only argue that *if* the legislator chooses (like the EU legislator has done) to make the right to data protection a fundamental, unalienable right, *then* data ownership and a data economy based on personal data as a commodity are difficult to reconcile.[6] In summary, we will conclude that the EU fundamental right to data protection is at odds with trade in personal data, basically because it disqualifies personal data as a commodity. This is not a problem in itself, but building an economy on something that does not qualify as a commodity is problematic.

This paper is structured as follows. In Section 2, we further investigate the workings of existing business models in which people pay with their personal data, explain why in the EU data ownership does not exist (contrary to, for instance, the United States and China, in which data ownership does exist), and examine the EU strategy for a Digital Single Market, aimed at the free flow of data to enhance the data economy. In Section 3, we discuss the inalienability of personal data and the right to personal data protection from a fundamental rights perspective (primary legislation) under the EU Charter of Fundamental Rights. In Section 4, we discuss the inalienability of personal data and data subject rights from a data protection law perspective (secondary legislation) under the EU General Data Protection Regulation (GDPR). In Section 5, we provide conclusions.

2. Paying with your data

2.1. *Business models*

In order to understand at which conditions EU law can allow "trade" of personal data, we first clarify what "trading data" means and then differentiate amongst relevant scenarios. Regardless of the lack of specific declarations about the alienable/inalienable nature of personal data and the inalienable nature of personal data rights, as affirmed in earlier work,[7] we consider here that trading data means *obtaining or providing personal data in exchange for money, products or services* (digital services, other valuable information, etc.). From this perspective, we address two different scenarios: (a) the data controller asks personal data to the data subject in exchange for money or a valuable service (we will call this scenario: *primary personal data trade*); (b) the data controller exchanges personal data with a third recipient (e.g., a business, that can thus be-

[1] Malgieri, G., and Custers, B. (2018) Pricing privacy: the right to know the value of your personal data, Computer Law & Security Review, Vol. 34, Nr. 2, p. 289–303.

[2] E. Steel, C. Locke, E. Cadman and B. Freese, *How much is your personal data worth?' Financ. Times* (12 June 2013) <https://ig.ft.com/how-much-is-your-personal-data-worth/>accessed 6 November 2020. See also law and economics studies, e.g., Bilyana Petkova and Philipp Hacker, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers' [2016]Lecturer and Other Affiliate Scholarship Series <https://digitalcommons.law.yale.edu/ylas/13>.

[3] See Digital Content and Digital Service Directive (EU) 2019 /770, Article 3(1).

[4] See, indeed, V. Janeček and G. Malgieri, Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21 German Law Journal <https://papers.ssrn.com/abstract=3466089>accessed 19 December 2019.

[5] On this point, see largerly ibid; G. Malgieri and V. Janeček, '*Data extra commercium*' in S. Lohsse, R. Schulze and D. Staudenmayer (ed), *Data as Counter-Performance—Contract Law 2.0?* (Hart Publishing/Nomos 2020) <https://papers.ssrn.com/abstract=3400620> accessed 6 January 2020.

[6] Obviously, this could be used by those siding on the 'against personal data ownership' as an argument in their favour, by stating that it would be very hard to introduce personal data ownership in the EU, since it requires changing the EU Charter on fundamental rights and removing from this list the fundamental right to personal data protection. We agree this would be complicated, but, in essence, it is not impossible. 2000.

[7] Malgieri and Janeček (n 6).2020.

come a second data controller) in exchange of money (we will call this scenario: *secondary personal data trade*).[8]

The first scenario is mostly clear to people. When asked, most people think that free online services such as search engines (Google, Yahoo, etc.) and social media (Facebook, Twitter, LinkedIn, etc.) are based on business models that generate revenue via advertising, which users are confronted with when online. An increasing number of people also understands that revenues are generated via the exchange and trade of data. The exchange and trade of data may also result in advertising (e.g., on the same website or other websites), but it can also be used for other purposes, such as profiling, making predictions or automated decision-making. How this is done, for instance, which data are collected about them and how such data is processed, is not clear to most people though.[9] Despite concerns that people have about their privacy, most people keep using services that collect and process their personal data (the so-called privacy paradox).[10]

The second scenario is what follows after people have provided their personal data to data controllers. These tech companies use different strategies to generate revenue from large amounts of data. The main strategies are selling copies of the data, leasing the data or extracting further value from the data. Selling copies of the data is the easiest and most straightforward strategy. If data is considered the raw material, information the semi-finished product and knowledge the final product, selling copies of data is basically making the raw material available to others who can distil knowledge from it, sometimes combining datasets from different sources. Like many other raw materials, most datasets sell at very low prices.[11] Note that copies of datasets can be sold many times to different buyers. In order to extract more monetary value out of data, it may be interesting for data controllers to lease their datasets, for instance, via subscriptions. Instead of a one-time payment, this may generate monthly payments. When the data are very volatile, i.e., changing rapidly, it may easily get outdated. For data processing organisations, it may be interesting to have direct access to real-time, up-to-date data via lease constructions instead of buying static datasets. For companies offering such subscriptions, the costs may be higher though, because they may have to maintain their datasets and dataflows, helpdesks, etc.

The strategy to extract further value from datasets is the most complicated, but may generate the most revenue. This is the domain of extracting new knowledge, which is done with tools like data mining and machine learning.[12] It may also result in profiling.[13] The new knowledge can subsequently be used in many different ways. For instance, personalisation and customisation on the basis of user profiles may incite people to pay for online services. Also, it can be used to identify which people are interested in which products and services and when they are more inclined to purchase products and services.

2.2. *Data ownership*

In the EU, data ownership of personal data does not exist.[14] People or companies can own hardware devices on which personal data are stored, but not the personal data itself. To avoid any misunderstandings: in the EU legal framework, data can be owned, but there is no legal recognition of the ownership of *personal* data. Data ownership exists in the area of intellectual property rights and there even exist sui generis property rights for databases that do not qualify for other copyrights.[15] Even though personal data ownership does not exist in the EU, it can coexist with personal data protection regimes, as is the case in countries like the United States[16] and China.[17] Some authors[18] argue that personal data ownership should also be introduced in the EU, whereas others are hesitant or argue

[8] *In economic terminology, this distinction can also be understood as business-to-consumer (B2C) and business-to-business (B2B) respectively*. Since we focus on the legal aspects, we do not use this terminology. 2000

[9] B. Custers, S. Van der Hof, B. Schermer (2014) *Privacy expectations of social media users: the role of informed consent in privacy policies*, *Policy Internet*, Vol. **6**, No. 3, p. 268–95.

[10] P.A. Norberg, D.R. Horne, and D.A. Horne (2007) *The privacy paradox: personal information disclosure intentions versus behaviors*, *J. Consum. Aff.*, Vol. **41**, No.1, p. 100–26.

[11] E. Steel, C. Locke, E. Cadman, and B. Freese (2013) *How much is your personal data worth?*, *Financ. Times*, 12 June 2013, http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz2z2agBB6R; see also Steele, E. (2013) Financial worth of data comes in at under a penny a piece, Financial Times, June 12, 2013.

[12] T. Calders & B.H.M. Custers (2013), *What is data mining and how does it work?*. In: Custers B.H.M., Calders T., Schermer B., Zarsky T. (red.) *Discrimination and privacy in the information society*. nr. 3 Heidelberg: Springer.

[13] M. Hildebrandt, S. Gutwirth (2008) Profiling the European citizen. Heidelberg: Springer; Harcourt, B.E.: (2007) Against Prediction: Profiling, Policing and Punishing in an Actuarial Age. Chicago: University of Chicago Press.

[14] N. Purtova (2017) Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency, 10(2) Journal of Law and Economic Regulation November 2017; Purtova N. (2014) Default entitlements in personal data in the Proposed Regulation: Informational Self-Determination Off the Table … and Back on Again? 30(1) Computer Law and Security Review, 6; Dorner, M. (2014) Big Data und "Dateneigentum"' 9 Computer und Recht 617; Grützmacher, M. (2016) Dateneigentum – ein Flickenteppich, 8 Computer und Recht 485; Hören, T. (2014) Big Data and the Ownership in Data: Recent Developments in Europe, 36(12) European Intellectual Property Review 751.

[15] See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[16] P. Schwartz (2004) *Privacy, property and personal data*, 117 Harvard Law Review 2056; Janger, E.J. (2003) Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy, 44 William & Mary Law Review. 1801.

[17] T. Fu (2019) *China's personal information protection in a data-driven economy: a privacy policy study of Alibaba, Baidu and Tencent. Glob. Media Commun.*, **15**(2), 195–213.

[18] See Nadezhda Purtova, Property Rights in Personal Data: A European Perspective (Kluwer Law Intl 2011); Nadezhda Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25 Computer Law & Security Review 507; Nadezhda Purtova, 'Illusion of Personal Data as No One's Property' (Social Science Research Network 2013) SSRN Scholarly Paper ID 2346693 <https://papers.ssrn.com/abstract=2346693>accessed 2 June 2019 See also Zech, H. (2015) Information as Property, 6 JIPITEC 192. Zech, H. (2015) Information as Property, 6 JIPITEC 192;

against this.[19] Personal data ownership can be complicated, as it may raise issues and complications similar to those well-known in the intellectual property rights domain. Typically, it can be complicated to describe what exactly is covered by the property rights, to assign ownership, and to enforce such rights, as information is easily copied and distributed.[20]

In this paper, we do not argue for or against the position of data ownership. We merely observe that it does not exist in the EU, but does exist in other jurisdictions. From that starting point, we analyse the consequences of the EU position. The fundamental right to personal data protection in the EU is unique in the world. It has some remarkable consequences when it comes to data ownership and existing free online business models, which will be discussed in the following sections.

With the absence of data ownership of personal data, but the possibility of data ownership of non-personal data, it becomes essential to determine the scope of personal data protection law and the concept of personal data. The EU has created a fundamental right to the protection of personal data, unique in the world, which is described in Article 8 of the Charter of Fundamental Rights of the European Union in a very general way: "everyone has the right to the protection of personal data concerning him or her". Whereas most nations offer constitutional protection of privacy, traditionally focused on protecting personal life and family life, the EU has added a separate right to the protection of personal data. The fact that the right to personal data protection is included in the list of fundamental rights in the EU makes it an inalienable right.[21] The inalienability of the protections offered in human rights law means that those protected by these human rights are not free to renounce them, even if voluntarily.[22]

If data match the definition of personal data, the GDPR provides specific rules and obligations for the collecting and processing of such data. Personal data can only be collected and processed if there exists an explicit legal basis for this, such as consent or a contract, see Section 4.1. The GDPR does not assign ownership of personal data to particular actors. Still, data subjects have several rights regarding their personal data, including a right to transparent information on the data collected and the purposes for which it is processed (Articles 12–14), a right to access to their data (Article 15), a right to rectification (Article 16), a right to erasure (Article 17), a right to data portability (Article 20) and a right not to be subject to automated decision-making (Article 22). As will be discussed in Section 4.1, these rights are inalienable, i.e., they cannot be waived, renounced, or transferred by data subjects. Neither does the GDPR accept any assigning or mandating of these data subject rights to others.[23]

Via the EU fundamental right to data protection and the data subject rights the GDPR provides, it becomes clear that (a) (legal) ownership of personal data is not recognised in the EU and (b) personal data rights are inalienable.[24] This means that when companies offer free products and services online in return for data, the concept of 'paying with your data' is something of a misnomer, as it is impossible to pay with your data because you cannot give what you do not own. From a legal perspective, it may be argued that 'paying with your data' should not be interpreted as a transfer of full and exclusive ownership of the data, but merely as a transfer of rights derived from ownership, i.e., encumbrances, such as granting access and processing rights to your data.[25] Granting such rights as payment for any free online products or services basically boils down to granting use rights, often via licensing. Although this legal description comes close to the actual transactions that take place when 'paying with your data', there is one major issue, however. That is that encumbrances and user rights, once vested, normally cannot be revoked at will by the person who granted them. As will be discussed in the following sections, the EU legal framework for personal data protection and the inalienability of personal data and personal data rights allow data subjects to revoke such rights after they granted them at any time and at will, causing considerable legal uncertainty in transactions, particularly on the side of data controllers.

2.3. *The EU digital single market*

One of the current major goals of the EU is to create a Digital Single Market.[26] In 2015, the EU launched its strategy to expand the European Single Market consisting of the 'four freedoms' (i.e., free flow of goods, capital, services, and labour) with a fifth freedom, i.e., a free flow of data. The three main elements of this strategy are access to online products and services, conditions for digital networks and services to grow

[19] A. Wiebe (2017) *Protection of industrial data – a new property right for the digital economy? 12(1)* J. Intellect. Prop. Law Pract. 62; Hugenholtz, B. (2018) Against Data Property, in Hans Ullrich, Peter Drahos and Gustavo Ghidini (eds), Kritika: Essays on Intellectual Property (Volume 3, Edward Elgar Publishing Limited; Drexl, J. (2017) Designing Competitive Markets for Industrial Data in Europe – Between Propertisation and Access, 8 JIPITEC 257.

[20] V. Janeček, '*Ownership of personal data in the internet of things*' (2018) **34** Comput. Law Secur. Rev. 1039.

[21] Contrary to the Universal Declaration of Human Rights, the EU Charter is not explicit about the inalienability of fundamental rights. Nevertheless, it is generally assumed that inalienability is at the essence of fundamental rights. See Malanczuk, P. (1997) Akehurst's modern introduction to international law, Routledge, London. See also the preamble of the 1948 Universal Declaration of Human Rights that suggests that the "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world". Universal Declaration of Human Rights (1948), GA Res. 217 A (III).

[22] D. Groome (2011) *Chapter 1: overview of human rights law. handbook of human rights investigation*, Penn State University.

[23] Article 80 of the GDPR provides data subjects with the right to mandate privacy organizations to lodge complaints on their behalf. But this only applies to the right lodge a complaint and the right to an effective remedy, not to the data subject rights in Chapter 3 of the GDPR. 2000.

[24] Or, as sometimes argued, personal data is subject to a dynamically limited alienability rule, see Malgieri and Janeček (n 6); Janeček and Malgieri (n 5).2000.

[25] A complication of this argument is that if no ownership exist, technically speaking also no secondary rights can be derived from it. Therefore, such rights would have to be sui generis rights.2000

[26] COM (2015) 192 final, A Digital Single Market Strategy for Europe, Brussels, 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

and thrive, and the growth of the European digital economy. The underlying goal of the strategy is to enhance the EU's data economy, ensuring the EU's competitiveness in the global economy.

The strategy is elaborated in many forms of secondary legislation. For instance, in 2018, the EU adopted Regulation 2018/1807 on the free flow of non-personal data in the EU.[27] The GDPR, which is often assumed to only focus on the protection of data subjects, has also aspirations in this direction, as can be read in its full title ("on the protection of natural persons with regard to the processing of personal data *and on the free movement of such data*") and its objectives defined in Article 1 ("This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data *and rules relating to the free movement of personal data*"). As such, the EU's legal framework for personal data protection is torn between two ideas (i.e., restricting data flows to protect people versus encouraging data flows to enhance the data economy).[28] Disqualifying personal data as a commodity is not a problem in itself, but building an economy on something that does not qualify as a commodity is problematic.

That this is problematic is supported by two observations. The first observation is that the EU does not have any of the data-crunching big tech companies like the ones based in the US and those emerging in China.[29] That could be due to the fact that the EU is not a single country like the US or China or because US big tech companies already dominate the EU market,[30] but it could also be due to the restrictions in the current legal framework. The second observation is that many companies seem to find it hard to comply with the current legal frameworks, most notably the GDPR,[31] something the EU has also admitted.[32] Taking these observations together, one may wonder whether the current legal framework is actually impeding the development of an EU data economy rather than facilitating it. The intended economic goals of the EU legal framework, such as a Digital Single Market and the free flow of data, do not (yet) seem to fully materialise. In fact, to some extent the current legal framework may even be counterproductive with regard to these goals, as some of the big tech companies are leaving or threatening to leave the EU market because of the data protection rules and the hefty fines that can be imposed.[33] Another practical consideration is that companies active both inside and outside the EU may be required to provide personal data to public authorities of non-EU countries, such as law enforcement authorities, which may be a violation of the GDPR if this concerns personal data of EU citizens.[34]

It seems that the EU is starting to realise this incongruency, as there is increasing discussion on the topic within the EU, particularly in the area of consumer law. In the past, consumer law has not been applied much to 'free' services, i.e., services that are not rendered against a monetary price often fell outside the scope of consumer law .[35] However, the provisions in the Unfair Commercial Practices Directive[36] and the Digital Content Directive[37] are phrased in such a way that they can also be applied to 'free' services. The European Commission confirmed this in its guidance.[38] Thus, it seems to be increasingly assumed in EU consumer law that data subjects can trade their personal data as a commodity. This acknowledges the economic reality that many digital services are offered not in exchange for a monetary payment, but in exchange of personal data. Particularly the Digital Content Directive seems to adapt legal reality to that economic reality.[39]

These discussions show that policymakers are struggling with this, but also that the existing incongruencies have not yet been solved. In the following sections, we focus on the inalienable nature of personal data rights (both in the EU Charter of Fundamental Rights and the GDPR), which are at odds with actual business practices and with the EU's envisioned data economy examined in this section.

[27] Regulation (EU) 2018 /1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, https://eur-lex.europa.eu/eli/reg/2018/1807/oj

[28] See also T. Zarsky (2017) *Incompatible: the GDPR in the age of big data*, *Seton Hall Law Rev.*, Vol. **47**, Iss. 4, Article 2.

[29] A. Renda (2020) *Europe's big tech contradiction*, *Cent. Eur. Policy Stud.*, 2 April 2019, https://www.ceps.eu/europes-big-tech-contradiction/#_ftn1.

[30] A.P. Jurak (2020) *The importance of high–Tech companies for EU economy–Overview and the EU grand strategies perspective*. *Res. Soc. Change*, **12**(3), 32–52.

[31] S. Mendoza (2018) *GDPR compliance-it takes a village*. Seattle UL Rev., **42**, 1155; Sirur, S., Nurse, J. R., & Webb, H. (2018) Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (p. 88-95); Kutyłowski, M., Lauks-Dutka, A., & Yung, M. (2020). GDPR challenges for reconciling legal rules with technical reality. In *European Symposium on Research in Computer Security* (p. 736-755). Springer, Cham.

[32] J. Espinoza (2020) EU admits it has been hard to implement GDPR, Irish Times, 23 June 2020. https://www.irishtimes.com/business/technology/eu-admits-it-has-been-hard-to-implement-gdpr-1.4286207.

[33] M. Lynn. (2022) Why the EU should fear an exodus of Big Tech companies, MoneyWeek, 20 February 2022. https://moneyweek.com/investments/stocks-and-shares/tech-stocks/604461/why-the-eu-should-fear-an-exodus-of-big-tech. Deutsch, J. Bodoni, S. (2022) Meta Renews Warning to EU It Will Be Forced to Pull Facebook, Time, 8 February 2022. https://time.com/6146178/meta-facebook-eu-withdraw-data/

[34] S. Carrera, G.G. Fuster, E. Guild, & V. Mitsilegas (2015) Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights. Brussel: Centre for European Policy Studies.

[35] N. Helberger, F. Zuiderveen Borgesius, A. Reyna (2017) *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, *Common Mark. Law Rev.* **54**, p. 1427–66.

[36] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, O.J. 2005, L 149.

[37] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[38] Commission Guidance on Directive 2005 /29/EC, *cited supra note 5, at 37, with reference to Case C-281/12, Trento Sviluppo srl,* Centrale Adriatica Soc. Coop. Arl v. Autoritate Garante della Concorrenza e del Mercato, EU:C:2013:859, paras. 36 and 38: "any decision directly related to that decision".

[39] N. Helberger, F. Zuiderveen Borgesius, A. Reyna (2017) *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, *Common Mark. Law Rev.* **54**, p. 1427–66.

3. Inalienability under the EU charter of fundamental rights

3.1. *The fundamental right to data protection*

The need for a right to protection of personal data significantly increased with the emergence of information and communication technology in the second half of the twentieth century. Historically, a right to data protection was considered as an aspect of the right to privacy. This has also been referred to as the right to informational privacy (as opposed to or complementary to spatial, physical and relational privacy).[40] In order to further protect personal data, countries (mostly EU member states) created data protection legislation. The German state of Hesse enacted the first Data Protection Act of the world in 1970. The first national data protection acts include the Swedish Data Act of 1973, the Austrian Data Protection Act of 1978, and the Norwegian Act relating to Personal Data Registers of 1978. Only in 1995, the EU harmonised data protection law via Directive 95/46/EC and firmly strengthened this harmonisation in 2016 with the General Data Protection Regulation (GDPR), which will be discussed in the next section.

However, all this legislation is secondary legislation, which does not explicitly mention a *fundamental* right to data protection (apart from the GDPR). Instead, in the fundamental rights context, the right to data protection was always assumed from the right to privacy, most notably mentioned in Article 8 of the European Convention of Human Rights (ECHR), see for instance, the case *Z versus Finland* (1997 25 E.H.R.R 371). In the EU, the Court of Justice of the EU (CJEU) traditionally strongly relies on the ECHR for guidance regarding human rights. Only after the Charter of Fundamental Rights of the EU (the Charter), drafted in 2000, came into force in 2009 via the Treaty of Lisbon, this provided the CJEU with another source of guidance regarding fundamental rights. Over time, with each legislative reform, the right to data protection has been gradually further disconnected from the right to privacy and the right to data protection has been regulated on a higher level, eventually even being adopted in the list of fundamental rights.[41]

Despite the long-time absence of its codification, a fundamental right to data protection has existed in EU case law for a long time. The CJEU recognised the right to protection of personal information as a general principle in EU law as early as 1969 in the case of *Stauder* versus *the City of Ulm* (Case C-29/69).[42]

With the adoption of the Charter, a fundamental right to personal data protection was explicitly included in the list of fundamental rights that EU citizens have. Article 8 of the Charter states that everyone has the right to the protection of personal data concerning him or her. This has legally binding force. In principle, the elevation of personal data protection to the category of an EU fundamental right could appear to constitute a decisive reinforcement of the level of protection effectively granted to individuals throughout the EU.[43] However, some have argued that the right to data protection enshrined in the Charter does not meet the criteria for fundamental rights and should be considered as an ordinary consumer right.[44] For instance, Article 8 of the Charter (contrary to any other fundamental rights listed in the Charter) explicitly mentions independent supervision (in practice by national data protection authorities), a provision that is further detailed with roles and task descriptions in the GDPR.

3.2. *The inalienability of fundamental rights*

Regardless of the question of whether the right to data protection in the Charter should be a fundamental right and the question of what it encompasses, it is clear that, by its incorporation in the Charter's list of fundamental rights, it is at this stage without doubt a fundamental right. Given that the right to data protection is a fundamental right in the EU, there are a few apparent conclusions that can be drawn. Typically, fundamental rights are inherent (i.e., they belong to people simply because they are human, they do not have to be bought, earned or inherited), basic (i.e., they provide minimum levels for human dignity), inalienable (i.e., they cannot be taken away), imprescriptible (i.e., they do not expire and cannot be lost, not even after longer times), indivisible (i.e., they cannot be denied when other rights have already been enjoyed), universal (i.e., they are irrespective of someone's origin, status, gender, etc.) and interdependent (i.e., the exercise of one right is connected to other rights).[45]

Here we want to particularly focus on the inalienable nature of fundamental rights. The inalienability of a fundamental right means it cannot be taken away. No one has the right to deprive another person of a fundamental right for any reason. People have fundamental rights, even if they are sometimes violated. The inalienable nature of fundamental rights is twofold: first, they cannot be rightfully taken away from someone and, second, they cannot be given away, transferred or be forfeited. Now that data protection is a fundamental right, this means it cannot be taken away, even if others (for instance, social media, data brokers, etc.) intentionally or unintentionally interfere with this. Also, it cannot be given away, even if some people are very sloppy with their personal data

[40] For a detailed analysis of the emergence of data protection as a fundamental right see largely Gloria Gonzalez Fuster, *The emergence of personal data protection as a fundamental right of the EU* (Springer International Publishing 2014) <https://www.springer.com/gp/book/9783319050225>accessed 20 May 2020.

[41] B. Sloot (2017) *Legal fundamentalism: is data protection really a fundamental right?* in: R. Leenes, R. van Brakel, S. Gutwirth, P. de Hert (eds.) *Data protection and privacy: (In)visibilities and infrastructures*. Heidelberg: Springer.

[42] https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:61969CJ0029.

[43] G. González Fuster, & R. Gellert. (2012) *The fundamental right of data protection in the European Union: in search of an uncharted right*, *Int. Rev. Law Comput. Technol.*, **26**:1, 73–82.

[44] B. Sloot (2017) *Legal fundamentalism: is data protection really a fundamental right?* in: R. Leenes, R. van Brakel, S. Gutwirth, P. de Hert (eds.) *Data protection and privacy: (in)visibilities and infrastructures*. Heidelberg: Springer.

[45] E.L. Cf. Rubin (2003) *Rethinking Human Rights, International Legal Theory 9(1); Alston, Ph. (1999) The EU and Human Rights*. Oxford: Oxford University Press.

and agree to hand over all kinds of personal data online (for instance, in exchange for free online services like search engines and social media).

It is important to note the difference between the inalienability of the right to personal data protection and the inalienability of any personal data itself. The latter is important for the extent to which personal data can be owned and can be considered as a commodity. From a legal perspective the right to personal data protection is inalienable, but strictly speaking, this is not the case for personal data, at least not explicitly. Property rights should not automatically be connected to the possibility to waive or alienate them. It can be argued that the right to data protection prevents the commodification of personal data.[46] But for those who do not agree with this argument on the inalienability of personal data, we point out that already the inalienability of personal data *rights* stands in the way of the commodification of personal data.

The fundamental right to personal data protection has a strong link with human dignity.[47] In particular, dignity presupposes the free development of personality through self-determination and self-flourishing, two principles that many authors consider the rationale for privacy protection.[48] Also within the German Federal Constitutional Court's doctrine on the existence of a general right to personality, some commentators noticed the link between personality, human dignity and privacy.[49] Moreover, the German Federal Constitutional Court had already suggested that the protection of persons against the processing of personal data was falling under the right to human dignity, as mentioned in Article 1(1) of the Fundamental Law, read in conjunction with its Article 2(1), on the free development of personality.[50] Interestingly, in more recent national constitutions in European countries, the concept of dignity and the concept of privacy and data protection are often connected.[51] Also, in the Italian Data Protection Law in 1996 (and in the modernised version of 2003), Article 1 declared that the goal of that data protection law was also the protection of dignity.

The link between data protection and dignity implies the inalienability of such protection[52] and, as we will argue in the next section, the inalienability of all data subject rights (including the right to withdraw consent to the processing of personal data).

4. Inalienability under the GDPR

4.1. *Data processing restrictions under the GDPR*

The General Data Protection Regulation (GDPR) came into force in 2018 and is an EU regulation, a legislative instrument that is directly binding for all EU Member States and its citizens.[53] It replaces the EU Data Protection Directive of 1995, a legislative instrument that needed to be implemented in national legislation by each EU Member State. To a large extent, the directive carried over the OECD idea of a set of fundamental data protection principles. In essence, the GDPR builds on the provisions in the EU Directive it replaces, but further strengthens several data subject rights (such as the right to data portability and the right to be forgotten)[54] and introduces some new concepts (such as data protection impact assessments, privacy by design and data breach notifications).[55]

Under the GDPR, data traders need to have a legal basis for the commercial exchange of personal data. Legal bases for processing personal data are listed in Article 6 GDPR.[56] Excluding the possibilities to 'monetise' data on the basis of a legal obligation, vital interest or public duty (mentioned in Article 6.1, under c, d and e), we will focus on consent, contract and legitimate interests (mentioned in Article 6.1, under a, b and f).

[46] The analogy between slavery and data protection is increasingly used in some literature, under the term 'data slavery', cf. Hildeabandt, M. (2013) *Slaves to Big Data. Or Are We? 17 IPD Revista de Internet, Derecho y Politica*, p. 7–44.

[47] D. Damanhouri (2017) *Data slavery: you're actually selling your information for free*, Medium.com, 3 November 2017; Pirkowski, M. (2018) Data Slavery and Decentralized Emancipation: Facebook, Google and the Future of Data Ownership, *Medium.com*, 21 June 2018.

[48] Lee A Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Review 17, 18; Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York Law Review 962; Fuster (n 34) 23; Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307; James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 The Yale Law Journal 72.

[49] Bart van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?' (2014) 5 JIPITEC <http://www.jipitec.eu/issues/jipitec-5-3-2014/4097>; Antonio Enrique Pérez Luño, Derechos humanos, Estado de Derecho y Constitución (Edición: edición, Tecnos 2010) 324.

[50] See Fuster (n 34) 26.2000.

[51] Mikrozensus-Urteil, *16.07.1969 (1 BVerfGE 27, Rn. 20). See Paul de Hert and Serge Gutwirth, '"Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power"'* in E Claes, A Duff and S Gutwirth (ed), Privacy and the Criminal Law (Intersentia 2006) **80**; See also Fuster (n 34) 176.

[52] See the Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic, No. 2/1993 Coll. In that Charter, the same Article (Article 19) recognizes both a right to human dignity and a right to the protection of private life and protection against the unwarranted collection, publication, or other illicit uses of personal data. Analogously, see Article 19(1)-(3) of the 1992 Slovakian Constitution. See also that in the EU Charter of Fundamental Rights, even though the right to dignity (Article 1) is separate from the rights to privacy (Article 7) and data protection (Article 8), Rodotà co-authored an amendment clearly connecting data protection to the protection of identity, human dignity and confidentiality (see Amendment 373 (CHARTE 4332/00, CONVENT 35, 463).

[53] See, e.g., J. Waldron, *Dignity, Rank, and Rights* (Oxford University Press 2012) 140–1.

[54] European Parliament and Council Regulation (EU) 2016/679 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 (General Data Protection Regulation) [2016]OJ L 119.

[55] See Chapter 3 of the GDPR. 2000.

[56] See Chapter 4 of the GDPR. 2000

Consent can be a legal basis for collecting data for monetisation purposes.[57] However, according to Article 7 GDPR, this consent must be unambiguous, fully informed (about the commercial purpose of the data processing), revocable and free (not conditional upon the provision of services *with no other genuinely equivalent alternatives*). In this case, businesses who 'trade' personal data must check that consent has been unambiguously provided, that it was informed, free, and still valid. The consent is valid if it is free (e.g., equivalent alternatives to process personal data, such as a counter-performance for the provision of a service should be still available and genuinely equivalent) and if it has not been revoked by the data subject.

If the processing of personal data is based on consent, people can revoke this consent at all times and at will, without further explanation. The loss of consent by the occasional user is usually not an issue for large companies. However, the simultaneous revocation of consent by large amounts of users could be problematic for companies who have built their business models on personal data. In practice, people rarely revoke their consent,[58] which means that large-scale revocation of consent may not be realistic in practice. However, given that the legal framework allows for this possibility, it does create legal uncertainties for these companies.[59]

As an alternative to consent, one might wonder if the "necessity for the performance of a contract to which the data subject is party" (Article 6.1.b) can be a legal basis for monetising personal data. Commentators have excluded this possibility.[60] In addition, the Article 29 Working Party (WP29) has clarified that this "provision must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller". WP29 explicitly excluded the use of contract as a legal basis for processing data for monetisation purposes (in that particular case, for marketing purposes).[61]

The only remaining possibility for processing personal data for a monetisation purpose (apart from consent) might thus be the necessity "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" (Article 6.1.f). This legal basis requires the respect of several tests, including at least: (1) the necessity test; (2) the legitimacy test; and (3) the balancing test considering the counter-interests of the data subject.

The use of 'legitimate interest' for monetisation purposes is problematic,[62] especially considering the necessity test. WP29 has indeed clarified that data controllers should "consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller".[63] In data trade, the identified purpose might be "economic profit from personal data", but in that case, the purpose might be considered too general and vague.[64] In addition, the purpose of economic profit could be reached through less invasive means (e.g., in the case of content providers, they might provide 'premium' services upon payment).

The legitimacy test can be interpreted extensively,[65] but the interest must be always lawful, sufficiently clear and represent a real and present interest.[66] As regards the balancing test,[67] it should be based on the evaluation of: (a) controller's legitimate interest, (b) impact on the data subjects (e.g. intrusiveness of profiling), (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects (transparency, easiness to exercise the right to object, etc.).[68]

All these considerations make the use of "legitimate interest" as a legal basis for "trading" personal data extremely difficult. However, it will be necessary to evaluate on a case-by-case basis whether the trade of data involves intrusive profiling, unclear information about purposes or commercial implications, etc. A confirmation of this comes from recital 47 of the GDPR, which declares that the most emblematic case of processing data for a "monetisation purpose", i.e., direct marketing, "may be regarded as carried out for a legitimate interest". However, in that case, the data subject has the right to object at any time to that processing so that the personal

[57] For sensitive data there is an additional (stricter) list of cases listed in Article 9 of the GDPR. See also Gil González and Paul de Hert, "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles", (2019) 20 ERA Forum 1–25.

[58] See Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (2014, WP 217), p. 18. See also Borgesius, "Personal Data Processing for Behavioural Targeting: Which Legal Basis?", (2015) 5 International Data Privacy 163–176, at 176.

[59] B.H.M. Custers (2016) *Click here to consent forever; Expiry dates for informed consent*, *Big Datad Soc.*, pp. 1–6. 10.1177/2053951715624935.

[60] Furthermore, the business models of these companies are often mixed, including basic and premium services. While the number of premium users may be much lower than that of basic users, it could still be sufficient to sustain the company even if all basic users revoke their consent. 2000.

[61] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed. (Oxford University Press, 2007), pp. 234–235; Borgesius, op. cit. *supra* note 70, at 170.

[62] See Article 29 Data Protection Working Party, op. cit. supra note 51, p. 17: "[contract] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract".2000.

[63] Borgesius, op. cit. *supra* note 51, at 170.2000.

[64] See Article 29 Data Protection Working Party, op. cit. supra note 51, pp. 29 and 55.2000.

[65] See Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation* (2013, WP 203), p. 16, : "For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will—without more detail—usually not meet the criteria of being 'specific'.

[66] See Article 29 Data Protection Working Party, op. cit. *supra* note 51, p. 24.2000.

[67] ibid. p. 25.2000.

[68] See, in particular, Kamara and De Hert, "*Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach*" in Selinger, P and Tene (Eds.), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2018).

data shall no longer be processed for such purposes (Article 21.2 and 21.3 GDPR). Accordingly, even though the monetisation purpose had to pass the legitimate interest test, the data subject shall have an immediate right to object, which seems to be very similar to the right to revoke consent in case of processing based on consent.

In addition, if "traded data" are not only personal, but also "sensitive" (according to the definition of Article 9.1 GDPR) data, they can never be processed for merely legitimate interest purposes, since under Article 9, there is no reference to "legitimate interest" as a legal basis for processing. In that case, just two legal bases might be in principle adequate for processing sensitive data for a monetisation purpose: either the data subject has given "explicit consent for one or more specified purposes" (Article 9.2.a GDPR) where consent must be, of course, also free, informed and revocable as described at Article 7 GDPR, or the processing relates to sensitive "data which are manifestly made public by the data subject" (Article 9.2.e GDPR). In this last case, however, we observe that if personal data are already public, their commercial value for data traders might be minimal (they would not need to 'buy' these data, they just would need technological resources to efficiently collect such data). Even in this second case, we remind that for processing sensitive data, controllers need to have a legal basis not only under Article 9 but also under Article 6 (since sensitive data are personal data anyway).[69] Therefore, in the case of processing of sensitive data which were manifestly made public by the subject, the data controller should either seek the consent of the subject under Article 6.1.b or prove that there is necessity for a legitimate interest under article 6.1.f. In the latter case, it appears extremely difficult that the controller could pass the aforementioned legitimacy test, necessity test and especially the balancing test when trading sensitive data for merely commercial reasons (in exchange of money).[70]

As regards secondary data trade, i.e., the monetised exchange of data between two data controllers (for instance, between a service provider and an advertising company), the same aforementioned conditions apply. In addition, in the case of consent, it might be necessary to collect separate consent for exchanging data with a third party. The WP29 has clarified that, in order to respect the principle of 'granularity', the data controllers that process data for their own purposes must ask for separate consent to communicate the data to a third party (e.g., an advertising company).[71]

In summary, consent is the most obvious legal basis for trading data and for letting people 'pay with their data' for online products and services, but consent is also uncertain and dynamic. Even if data "traders" pass the "freedom of consent" test, consent could be revoked at all times, at will, in the future.[72] Legitimate interest is an extremely difficult basis for trading data: data controllers first need to pass the necessity, legitimacy and balancing tests, but even if that succeeds, the data subject could easily object (Article 21 GDPR) and so block the data processing. Contract is also a clear and possible legal basis, but then the same more or less applies as for consent. For instance, entering into a contract is usually also based on consent. After entering into a contract, national consumer law may allow data subjects to withdraw at all times. But regardless of consumer law provisions, the legal rights data subjects have according to the GDPR may conflict with any contractual legal basis for data processing, as will be discussed in the next subsection.

4.2. *The inalienability of data subject rights*

The inalienability of the fundamental right to personal data protection perpetuates in the GDPR, which has as a starting point the idea of informational self-determination. This concept was first developed in the 1960s, when it was argued that each person should have a right to determine for himself when, how and to what extent information about him or her is communicated to others.[73] This approach puts personal autonomy and informed consent central. The term *informational self-determination* was only first used in 1983 in a landmark ruling of the German Constitutional Court.[74] As a result, the GDPR contains many data subjects' rights that can also be considered inalienable and can influence the processing of personal data that was provided to or collected by data controllers.

Interestingly, the GDPR does not seem to accept that data subject rights can be assigned, mandated or delegated to others. In particular, Article 80 about the new figure of the "representation of data subjects" does not provide that representatives of data subjects may exercise on their behalf also the data protection rights (access, rectification, objection, erasure, portability, limitation). The representative's role is limited to judicial actions (Articles 77–79 GDPR) and the right to receive compensation. Although the possibility to mandate data protection rights is not explicitly excluded in the GDPR, accord-

[69] Article 29 Data Protection Working Party, op. cit. supra note 51, p. 33. 2000.

[70] See Article 29 Data Protection Working Party, op. cit. supra note 51, p. 15: "Publicly available data are still personal data subject to data protection requirements, including compliance with Article 7 [of the Data Protection Directive, now Article 6 of the GDPR], irrespective whether or not they are sensitive data, 2020".

[71] See Article 29 Data Protection Working Party, op. cit. supra note 51, p. 35 which – in the explanation of scenario n. 3 – affirms that when processing data for purely consumer profiling reasons "the inference of sensitive data (health data) […] contributes to tipping the balance in favour of the data subject's interests and rights". See, similarly, the example at page 59 (On-line pharmacy performing extensive profiling). See more in general, Ibidem, p. 38-39 which, while assessing the parameters of "nature of data" and "the way data are processed" in the balancing test, affirms that processing sensitive data (or even data that could reveal sensitive data) contributes to set the balance test in favour of the data subject (because "the more sensitive the information involved, the more consequences there may be for the data subject") 2020.

[72] Article 29 Data Protection Working Party, op. cit. *supra* note 51, p.10 2020.

[73] In this case the processing of data before withdrawal is not unlawful (Article 7(3) GDPR), but no new processing of such data is allowed. *At the same time, if there are no more legal bases, such data should be erased (see European Data Protection Board, Opinion 3/* 2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (Art. 70.1.b), p. 7).

[74] A. Westin (1967) Privacy and Freedom. London: Bodley Head

ing to some scholars, the data protection rights (Articles 15–22 GDPR) are neither "mandatable" nor exercisable by other persons apart from the data subject.[75] In private law, individual rights can be mandated or delegated to other subjects (e.g., legal representatives), but several scholars have excluded the applicability of private law rules in the data protection sphere considering the 'fundamental rights character' of data protection rights.[76] Although case law has not provided clarity on this matter,[77] these are indications that it is not possible to alienate such rights, including the right to withdraw consent (Article 7.3 GDPR), which appears the main obstacle against the pure alienation of personal data rights.

This is problematic for many of the free business models that are currently used. As explained above in Section 2, many social media companies, search engine companies, and other online services offer free services and base their business models on collecting and processing personal data for creating revenues (e.g., from selling or leasing the data or the knowledge resulting from data analytics). It is also the perception of users and the general public that they are 'paying with their data'. However, given that people do not own their personal data and have, according to the GDPR, inalienable personal rights (i.e., data subjects rights) over their personal data, from a legal perspective, they cannot pay with their data in the same way they usually pay with their money.

From the perspective of data controllers, this is problematic with regard to legal certainty. Even if people do not actually 'pay with their data', as argued above, it could still be argued that the 'payment' is more something like granting a right to collect and process the data to data controllers. However, even from that perspective, users would retain inalienable rights to stop or restrict the data processing at any time, without any further explanation. Compare this with buying a car: it would be strange if a customer, after buying a car and having paid it, takes the car and one month later also takes back the payment (without returning the car). Of course, it can be argued that, in the online environment, revoking consent to the data processing means that a user can no longer use the service from that moment on, like a newspaper subscription that stops if you cancel it (or stop paying for it). However, even that comparison does not entirely hold, since, under the GDPR, people can impose restrictions on the processing of their personal data in the form of data subject rights that cannot be waived. For instance, people can invoke the right to the erasure of their personal data (Article 17 GDPR) or the right to restriction of processing (Article 18 GDPR). Invoking such rights would not prevent them from enjoying the free online services, but obviously, invoking such user rights can strongly affect the value of the personal data for the data controller. This may cause considerable legal uncertainty in transactions, as it may change the agreed-upon transaction significantly in a later stage.

This legal uncertainty can be an issue at an individual level, for data controllers that enter into transactions, but also at the macro-economic level. The EU's envisioned data economy, pursued via its strategy for a Digital Single Market (see Section 2.3), largely depends on the free flow of data, including personal data. It assumes that personal data can be traded like a commodity, in line with actual practices. However, the data subject rights that the GDPR provides limit the extent to which personal data can be considered a commodity that can be freely traded. Building a data economy on the basis of this seems problematic.

5. Conclusion

The fundamental right to personal data protection guaranteed in Article 8 of the Charter on Fundamental Rights in the EU is unique in the world. No other jurisdiction in the world has elevated personal data protection to the level of a fundamental right. This is closely related to the introduction of the high level of data protection that the EU has tried to achieve with the adoption of the GDPR, generally accepted as offering the strongest (or at least one of the strongest) legal instruments for data protection worldwide.

However, the EU's choice of introducing the right to data protection in the catalogue of fundamental rights is not merely symbolic, but it has some considerable consequences. In this paper, we have argued that data protection as a fundamental right implies its inalienability; people cannot waive or transfer this right. This makes ownership of personal data and a data economy based on personal data as a commodity difficult to reconcile. In itself, that is not problematic since the EU never assumed or regulated data ownership of personal data.[78] Fundamental rights are not a commodity. Therefore, from a fundamental rights perspective, it makes sense not to allow the trade of personal data or any right to personal data protection.

Obviously, this is in sharp contrast with actual practices in the data economy.[79] Many companies build their free online business models on revenues based on the collection, analysis and trade of personal data that users provide in return for the services offered. People generally accept that these online services, such as social media and search engines, are for free because they 'pay with their data'. In other words, personal data is treated and traded by both companies and people as a commodity, even though the EU legal framework disqualifies personal data as a commodity.

[75] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfG 65, 1.

[76] S. Delacroix, . and N.D Lawrence. (2019) *Bottom-up Data Trusts: disturbing the "One Size Fits All" Approach to Data Governance International Data Privacy Law*, Vol. **9**, Issue 4, p. 236–52. https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz014/5579842; affirming that data protection rights cannot be mandated to third persons.

[77] O. Lynskey (2015) *The foundations of EU data protection law*, Oxford: Oxford University Press, p. 40.

[78] The CJEU, in in Case C–498/16, Maximilian Schrems v Facebook Ireland Limited, 25 January 2018, §49 affirmed that "assigning" rights under EU consumer law was not possible in the specific case at stake for jurisdictional reasons, but the Court did not discuss whether mandating consumer or data protection rights is forbidden or allowed.

[79] Note that the RU has discussed data ownership for a long time though. See A. Taranowski (2020) *EU drops data ownership*, Medium, 27 February 2020. https://medium.com/data-legally/eu-drops-data-ownership-807ca597fd62

The contrast between the legal framework stating that personal data is not and cannot be a commodity and actual business practices that treat personal data exactly as a commodity is remarkable.[80] It is also problematic, as it causes legal uncertainty in transactions, mostly because the legal basis for the processing of personal data is the consent of the data subject. Since the right to personal data is inalienable, people can at any time and at will revoke their consent for processing their personal data. Where normally all parties entering a transaction can agree on the payment for a service, the inalienable nature of personal data means that people can withdraw their payment after having received the services. Furthermore, even if they do not withdraw their consent entirely, they can limit the ways in which their personal data can be processed by invoking their (inalienable) data subject rights granted in the GDPR, such as the right to have data erased or restrict the processing of their personal data.

Furthermore, the EU's choice not to consider personal data as a commodity is in contrast with the EU's own goals regarding the creation of a Digital Single Market,[81] the EU strategy launched in 2015 to expand the European Single Market consisting of the 'four freedoms' (i.e., free flow of goods, capital, services, and labour) with a fifth freedom, i.e., a free flow of data. This strategy aims to strengthen the EU data economy. However, the EU's legal framework for personal data protection is torn between two ideas (i.e., restricting data flows to protect people versus encouraging data flows to enhance the data economy).[82] Disqualifying personal data as a commodity is not a problem in itself, but building an economy on something that does not qualify as a commodity is problematic. The EU does have an economy based on personal data, but one may wonder whether that is despite rather than due to the current legal framework. One indicator for this is that the EU does not have any of the data-crunching companies like the ones based in the US and those emerging in China.[83] That could be due to the fact that the EU is not a single country like the US or China or because US big tech already dominates the EU market,[84] but it could also be due to the restrictions in the current legal framework. Another indicator is that many companies seem to find it hard to comply with the current legal frameworks, most notably the GDPR,[85] something the EU has also admitted.[86]

We conclude that the fundamental right to personal data protection in the EU Charter of Fundamental Rights and the paradigm of the data subject rights in the GDPR are at odds with the practical reality of ubiquitous trade in personal data. This is not only a black letter law issue, but it also exposes ambiguous intentions of the EU legislator, that on the one hand wants to protect people and their personal data and does not want personal data to be considered as a commodity, but on the other hand, wants to build a data economy on the basis of personal data trade. Both are legitimate goals, but since it is impossible to have it all (at least through the current legal framework), it may be time for the EU to start making some choices here.

Data Availability

No data was used for the research described in the article.

[80] B.H.M. Custers, and D. Bachlechner. (2018) *Advancing the EU data economy; conditions for realizing the full potential of data reuse*, *Inf. Polity*, Vol. **22**, No. 4, p. 291–309. 10.3233/IP-170419.

[81] See also K.A. Bamberger, and D.K. Mulligan (2015), *Privacy On the Ground in the United States and Europe*, MIT Press; Custers, B.H.M., Sears, A.M., Dechesne, F., Georgieva, I.N., Tani, T., and Van der Hof, S. (2019) EU Personal Data Protection in Policy and Practice, Heidelberg: Asser/Springer. pp. 249.

[82] COM (2015) 192 final, A Digital Single Market Strategy for Europe, Brussels, 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

[83] See also T. Zarsky (2017) *Incompatible: the GDPR in the age of big data*, *Seton Hall Law Rev.*, Vol. **47**, Iss. 4, Article 2.

[84] A. Renda (2020) *Europe's big tech contradiction*, *Cent. Eur. Policy Stud.*, 2 April 2019, https://www.ceps.eu/europes-big-tech-contradiction/#_ftn1.

[86] A.P. Jurak (2020) *The importance of high–Tech companies for EU economy–Overview and the EU grand strategies perspective*. *Res. Soc. Change*, **12**(3), 32–52.

[86] S. Mendoza (2018) *GDPR Compliance-It Takes a Village*. *Seattle UL Rev.*, **42**, 1155; Sirur, S., Nurse, J. R., & Webb, H. (2018) Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (p. 88-95); Kutyłowski, M., Lauks-Dutka, A., & Yung, M. (2020). GDPR challenges for reconciling legal rules with technical reality. In European Symposium on Research in Computer Security (p. 736-755). Springer, Cham.