Spill-overs in data governance:
Uncovering the uneasy relationship between the GDPR's right to data portability and EU sector-specific data access regimes[1]

Inge Graef, Martin Husovec & Jasper van den Boom[2]

Abstract

A consensus is emerging that a flourishing European data economy requires effective portability of and access to data for individuals as well as businesses. Beyond the right to data portability introduced in the General Data Protection Regulation, a number of data access regimes are being developed in the energy, automotive, payment and digital content/services sectors. By comparing the key aspects of these instruments (including their objectives, scope, beneficiaries, configuration and modalities), the paper analyses the relationship of these sector-specific regimes with the right to data portability of the General Data Protection Regulation that applies to the entire economy. The paper identifies a set of possible unintended consequences – which we term 'spill-overs' – between these regimes in relation to how they govern data sharing in the EU. These spill-overs might be positive or negative for the welfare of society. They can be of factual or legal nature, and go both directions: from horizontal instruments to sectorial laws, and from sectorial to horizontal instruments. Some of the spill-overs are only a consequence of uncertainty and lack of clear direction. The existence of spill-overs highlights that a 'fragmented' legislative strategy pursuing horizontal and sector-specific data sharing policies in parallel can expand or contract the original goals/scopes intended by the legislator. As spill-overs take place irrespective of whether policy-makers consider them or not, legislators should be fully aware of them when they pursue a fragmented strategy for data sharing policies.

1. Introduction

While data is regarded as a key resource for economic growth and societal progress, policy makers are concerned that its full potential is not reaped as long as generators of data keep it to themselves and the information is consequently analysed in silos.[3] To promote the exchange and reuse of data across market players, the European Commission has been actively exploring policy options to address issues of data sharing. In particular, the Commission adopted a Communication 'Towards a common European data space' in April 2018 in parallel with a Staff Working Document taking the shape of 'Guidance on sharing private sector data'.[4] At the national level, the Dutch government for instance published a 'Vision document on data sharing between companies' in February 2019.[5] This increased attention to

[1] This research has been conducted in the framework of the research project 'Conceptualising Shared Control Over Data' that received funding from Microsoft. We would like to thank the editors and the anonymous reviewers for their very thoughtful comments that helped us to strengthen the paper. Any errors are our own.

[2] Tilburg Law and Economics Center (TILEC) and Tilburg Institute for Law, Technology, and Society (TILT).

[3] Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final, p. 2 and 8.

[4] Commission, 'Towards a common European data space' (Communication) COM (2018) 232 final; Commission 'Guidance on sharing private sector data' (Staff Working Document) SWD (2018) 125 final.

[5] Dutch Ministry of Economic Affairs, 'Nederland Digitaal - De Nederlandse visie op datadeling tussen bedrijven' [2019] <https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses> accessed 19 April 2019.

the issue of data sharing among businesses can be traced back to the adoption of the General Data Protection Regulation (GDPR)[6] which has introduced a right to data portability (RtDP) in Article 20. Data openness and transparency more broadly obviously have a much longer history, dating back to the open source movement of the early computer industry and the subsequent open culture and open data movement in the public sector.[7]

The focus of this paper is specifically on data sharing in business-to-consumer and businesses-to-business relations. The research question analysed is how different data access regimes relate to one another and can impact each other's interpretation, in particular considering the parallel application of the GDPR's RtDP, which applies horizontally across the economy, with newly developed sector-specific regimes for data access.[8] In other words, what overarching insights can be distilled from the current piecemeal approach of regulating data sharing across sectors? After careful analysis of existing instruments, we identify a set of 'spill-overs', which might occur from the implementation of sector-specific data access instruments for the interpretation of more horizontal regimes like the GDPR, and the other way round. We define a spill-over as an unintended impact that the substance of the rules in one regime might have on the interpretation of the rules in another regime, irrespective of their original meaning and policy goals. We aim to highlight that as wider accessibility and reuse of data becomes common practice in selected industries, market players, policy makers and regulatory authorities may be less hesitant to apply similar approaches across the economy building upon the lessons learned from sector-specific interventions, and that sector-specific interventions might be in turned influenced by horizontal regimes.

Single horizontal regime

The GDPR's RtDP consists of two elements in that it provides data subjects with: (1) a right to receive their personal data provided to a controller 'in a structured, commonly used and machine-readable format' and transmit those data to another controller (Article 20(1) GDPR); and (2) a right to have the personal data transmitted directly from one controller to another 'where technically feasible' (Article 20(2) GDPR). Although the former Article 29 Working Party (the EU data protection advisory body now replaced by the European Data Protection Board) adopted 'Guidelines on data portability' in April 2017,[9]

[6] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. Hereinafter cited as "GDPR".

[7] See in particular Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56; for further discussion see OECD, 'Open Government Data Report: Enhancing Policy Maturity For Sustainable Impact, OECD Digital Government Publishing, OECD Publishing (2018); Commission, 'Creating Value Through Open Data', European Data Portal (2015).

[8] The interaction of the GDPR's RtDP with EU competition law as well as with intellectual property protection falls outside the scope of this paper. For such an analysis, see Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359; Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 *European Law Review* 793; Gianclaudio Malgieri, ''User-provided personal content' in the EU: digital currency between data protection and intellectual property' (2018) 32 *International Review of Law, Computers & Technology* 118; Barbara Van der Auwermeulen, 'How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations' (2017) 33 *Computer Law & Security Review* 57.

[9] Article 29 Working Party, 'Guidelines on the Right to Data Portability', WP (2017) 242 rev.01.

there are still many uncertainties surrounding the scope of the GDPR's RtDP. In particular, it is not clear in what form or to what extent Article 20 GDPR gives data subjects control over their data.[10] Furthermore, scholars have debated the rationale behind the RtDP. Although it forms part of a data protection instrument and can be considered to promote individual control over personal data,[11] one can also see the RtDP as an instrument to stimulate competition and innovation in data-driven markets.[12] In any case, it is clear that the GDPR's RtDP has an effect beyond data protection by potentially reducing lock-in through enabling users to switch easily between services. The RtDP will likely also increase competition between data controllers and encourage the exchange and reuse of data across the economy.[13] In this sense, the GDPR's RtDP has similarities with sector-specific data access regimes in terms of impact – even though their objectives and scope differ.

Four sector-specific regimes

Sector-specific legislation on the topic of data access has been adopted or is being developed in different sectors. The paper analyses the scope of legislative instruments enabling data access in a number of industries and compares them with the GDPR's RtDP that applies horizontally, across all sectors of the economy. The selected sector-specific regimes are: (1) the Electricity Directive in the energy sector,[14] (2) the Regulation on access to vehicle repair and maintenance information in the automotive sector,[15] (3) the Payment Services Directive 2 in the payment sector,[16] and (4) the Digital

[10] For an in-depth discussion, see Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1359-1398.

[11] See Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 *European Law Review* 793, 809-810. Lynskey argues that the RtDP 'sits coherently within the data protection regime' because it promotes individual control over personal data by enhancing informational self-determination as 'a central objective of the EU data protection regime'.

[12] See Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1369-1370; Joseph Drexl, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' (2017) 8 *JIPITEC* 257, 286.

[13] Some however have contested the pro-competitive effect of the GDPR's RtDP, in particular because of the compliance burden for small and medium-sized controllers. See Peter Swire & Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 *Maryland Law Review* 335, 349-353.

[14] 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 [2019] OJ L 158/125. Hereinafter cited as "Electricity Directive".

[15] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information [2007] OJ L 171/1. Although this Regulation relates to non-personal data and therefore does not overlap with the GDPR that regulates the processing of personal data, ongoing discussions in the automotive sector involve the creation of a broader form of access to in-vehicle data that does include personal data (See Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 13.). Such new measures may build upon the existing regulatory framework for access to non-personal data so that it is worth pointing out its scope here.

[16] Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35. Hereinafter cited as "PSD2".

Content Directive in the digital content/services industries.[17] These sectors are chosen because legislation regarding data access has either already been adopted or the relevant policy discussions are in an advanced stage.[18] Each of these instruments form part of consumer and market law more broadly, but have their own objectives and focus on protecting particular interests. Debates concerning data sharing and the resulting legislative or policy interventions emphasise different aspects, which in turn require a different scope of protection. The Oxford Dictionary defines access as 'a right or opportunity to use or benefit from something'.[19] This linguistic definition already suggests that access has a number of dimensions. An opportunity can be merely factual, but a right implies a legal claim (either defensive or affirmative). An ability to benefit implies being in a position of a passive recipient, while an ability to use would involve active shaping of possibilities. In addition, data access can be configured in different ways: by empowering individuals to have access to data for use by another provider or by facilitating exchange of data among market players directly upon the consent of the individual. Despite differences in scope, the GDPR's RtDP and the sector-specific instruments apply and can be invoked in parallel.

The paper is structured as follows. The first part compares a number of key aspects of the different data sharing instruments ('data sharing' is used in the remainder of the paper as umbrella term referring to both data portability and data access). The second part discusses the interactions or overlap between the GDPR's RtDP and the sector-specific data access regimes in order to identify possible spill-over effects that will impact their mutual interpretation. Based on this analysis, the conclusion draws lessons for the future implementation and development of data sharing tools within EU legislation and policy across sectors. Although each sector has its own peculiarities, we illustrate that it is possible to establish an overarching and more horizontal approach to the governance of data sharing in the EU that would benefit individuals as well as market players who increasingly value data access.

2. Comparing the data access regimes

In order to draw a comparison between the GDPR's RtDP and the sector-specific data access instruments in the energy, automotive, payment services and digital content/services industries, the first part of the paper analyses the main aspects of these data sharing frameworks. The selected dimensions considered as key in analysing interactions are: (a) objectives; (b) scope of data and type of control; (c) beneficiaries; (d) configuration; (e) modalities; and (f) standardisation of the different instruments. This part of the paper maps the scope of the different regimes and therefore inevitably has a descriptive character. In the course of the comparison, more analytical insights are gradually identified, and then fully theorised into a set of spill-overs effects in Section 3. As will be shown towards the end of the analysis, despite the differences in scope of the sector-specific regimes at issue, spill-

[17] 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 [2019] OJ L 136/1.

[18] Another relevant instrument can be found in Article 6 of the Regulation on the free flow of non-personal data which empowers the Commission to encourage and facilitate the development of self-regulatory codes of conduct for porting non-personal data between cloud service providers (Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59). Because of its self-regulatory character and open scope, we do not discuss it in this paper.

[19] See Oxford Dictionary 'Access' [2019] <https://en.oxforddictionaries.com/definition/access> accessed 19 April 2019.

overs may occur that impact the interpretation of the GDPR's RtDP as a horizontal framework applicable across the economy.

2.1 Objectives

The objectives of a regulatory regime are key in determining and interpreting its scope, especially when it contains provisions with open norms. While the objectives of the different data sharing instruments overlap, there is no full alignment so that they can complement each other and provide for a more complete – but piecemeal – framework. The table below contains the objectives as they are mentioned in each of the instruments.

Legislation	**Objectives**
GDPR	Data protection, internal market for personal data
Digital Content Directive	Internal market; consumer protection
PSD2	Internal market for payment services
Electricity Directive	Internal market for electricity; energy efficiency; consumer empowerment
Regulation on access to vehicle repair and maintenance information	Internal market as regards free movement of goods, freedom of establishment and freedom to provide services in the market for vehicle repair and maintenance information services

The *GDPR* has a dual objective: (1) the protection of fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data; and (2) the protection of the free movement of personal data in the EU.[20] The GDPR is based on Article 16 of the Treaty on the Functioning of the European Union (TFEU), which establishes the principle that everyone has the right to the protection of personal data concerning them and was introduced as the new legal basis for the adoption of data protection rules by the Lisbon Treaty. In addition, the GDPR is the regulatory embodiment of the fundamental right to data protection as included in Article 8 of the EU Charter of Fundamental Rights. Beyond the fundamental right to data protection, the GDPR also furthers the integration of the internal market by protecting the free movement of personal data within the EU. In this regard, Article 1(3) GDPR states 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'. As a result, the GDPR is aimed at data protection but is not without due consideration of internal market objectives either.[21] The GDPR applies to all processing of personal data across the entire economy, including to the industries discussed here where sector-specific data access regimes have been or are being adopted.[22] It is this parallel application of the

[20] Article 1 GDPR.

[21] See also Nikolas Horn & Anne Riechert, 'Practical implementation of the Right to Data Portability', Stiftung Datenschutz 2017, p. 206-207.
Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1369-1370

[22] The material scope and a limited number of exceptions are laid down in Article 2 GDPR.

horizontal RtDP in the GDPR and sector-specific data access instruments that forms the study of this paper.

The relevant sector-specific regimes do not promote data protection as such. Instead, the regulatory frameworks in these sectors set out to stimulate the internal market, improve consumer protection, increase energy efficiency etc. However, although data protection is not an objective of these frameworks, their relationship with the GDPR is considered within the relevant Directives and Regulations to a greater or lesser extent.

As regards *digital content*[23] *and digital services*[24], the Digital Content Directive[25] in its Article 1 states that it aims 'to contribute to the proper functioning of the internal market while providing for a high level of consumer protection'. It does so by laying down common rules on certain requirements between suppliers and consumers such as the conformity with the contract, remedies in case of the lack of conformity or failure to supply, and the termination of long-term contracts. As regards data sharing, Article 16(4) of the Digital Content Directive lays down a data retrieval obligation for suppliers. In particular, the provision entitles consumers upon termination of the contract for the supply of digital content or digital services to retrieve any content other than personal data, which was provided or created by the consumer when using the digital content or digital service. Article 3(8) of the Digital Content Directive states that it is without prejudice to the GDPR and that the GDPR prevails in case of conflicts. In addition, Article 16(2) provides that traders have to comply with the obligations of the GDPR in respect of personal data of the consumer. Nevertheless, the Digital Content Directive has a complex relationship with data protection.[26] Although it aims to improve consumer protection by giving consumers the same rights when they enter into a contract for the supply of digital content whether they pay with money or with their personal data, the recognition of personal data as counter-performance has led to criticism from data protection advocates. In particular, the European Data Protection Supervisor has warned that the fundamental rights nature of the protection of personal data goes against the idea of personal data as a 'simple consumer interest' or a 'mere commodity'.[27] This tension between the two instruments may lead to uncertainties as to their parallel application in practice.

---

[23] Article 2(1) GDPR defines 'digital content' as: 'digital content' means data which is produced and supplied in digital form, for example video files, audio files, applications, digital games and any other software'.

[24] Article 2(1)(a) GDPR defines 'digital service' as: '(a) a service allowing the consumer the creation, processing or storage of, or access to, data in digital form (…); or (b) a service allowing the sharing of or any other interaction with data in digital form uploaded or created by the consumer and other users of that service'.

[25] Because the final version of the Directive was not yet available at the time of writing, we refer to the version adopted by the Council in June 2017: Council, 'General Approach of the Council' [2017] <http://data.consilium.europa.eu/doc/document/ST-9901-2017-INIT/en/pdf> accessed 19 April 2019.

[26] In the context of consent, see Damian Clifford, Inge Graef & Peggy Valcke, 'Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) 20 *German Law Journal* 679. For a discussion of the relationship between data protection and consumer law more generally, see Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54 *Common Market Law Review* 1427; and Dan Jerker B. Svantesson, 'Enter the quagmire – the complicated relationship between data protection law and consumer protection law' (2018) 34 *Computer Law & Security Review* 25.

[27] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' [2017], p. 3.

The *Payment Services Directive 2 (PSD2)*[28] lays down a so-called 'access-to-account' (commonly referred to as 'XS2A') rule in Articles 66 and 67 enabling third party providers to access a customer's payment account information on the customer's request in order to provide payment initiation or account information services. Recitals 27 and 28 refer to these new types of services as having emerged due to technological developments and consequently require to be included in the EU regulatory framework for payment services. In terms of objectives, recital 33 states that the PSD2 aims 'to ensure continuity in the market, enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework'. As such, the internal market objective prevails which is also illustrated by the fact that the PSD2 finds its legal basis in Article 114 TFEU, the provision used to enact harmonisation measures furthering the integration of the internal market. By creating clarity about the status of payment initiation and account information services, PSD2 can also be regarded as promoting competition and innovation in the payment sector through the explicit recognition of these services. As regards its relationship with data protection, recital 89 and Article 94(1) state that where the provision of payment services entails the processing of personal data, the EU data protection rules are applicable. Article 94(2) requires payment service providers to only 'access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user'. One needs to keep in mind that the GDPR was adopted after the PSD2, as a result of which the introduction of the access-to-account rule of the PSD2 precedes that of the GDPR's RtDP. However, while the provisions of the GDPR started to apply from 25 May 2018,[29] the ultimate compliance deadline for the access-to-account rule was 14 September 2019.[30] A relevant question that will be considered in section 3 below is how the access-to-account rule of the PDS2 and the GDPR's RtDP will influence each other (as both give rise to a form of data sharing). Even though the GDPR's RtDP inevitably interacts with the PSD2's access-to-account rule, the PSD2 does not engage with data protection apart from referring to the applicability of the data protection legislation.

This is different in the *energy sector*. The legislative instrument that is relevant in relation to data access is the Electricity Directive adopted in June 2019.[31] The Electricity Directive forms part of a broader package of initiatives entitled 'Clean Energy for All Europeans', which consists of Commission proposals to implement the Energy Union. It finds its legal basis in Article 194 TFEU, according to which the objectives of the EU's energy policy include ensuring the functioning of the energy market, security of energy supply, energy efficiency and the development of new and renewable forms of energy. As such, Article 1 of the Electricity Directive states that it aims to create 'truly integrated competitive, consumer-centred, flexible, fair and transparent electricity markets' in the EU. By using the advantages of an integrated market, the Directive, according to Article 1, aims 'to ensure affordable, transparent energy prices and costs for consumers, a high degree of security of supply and a smooth transition towards a

[28] Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35. Hereinafter cited as "PSD2".

[29] Article 99(2) GDPR.

[30] See Commission, 'Frequently Asked Questions: Making electronic payments and online banking safer and easier for consumers', 13 September 2019 <https://europa.eu/rapid/press-release_QANDA-19-5555_en.htm> accessed 3 October 2019.

[31] 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 [2019] OJ L 158/125. Hereinafter cited as "Electricity Directive".

sustainable low-carbon energy system', including through rules on consumer empowerment and protection, and on open access to the integrated market. Interestingly, the Electricity Directive pays special attention to data protection. In relation to smart metering and the processing of personal data, Article 20(c) requires that 'the privacy of final customers and the protection of their data' complies with 'relevant Union data protection and privacy rules'. In addition, Article 20(f) specifies that appropriate advice and information has to be given to final customers at the time of installation of smart meters concerning the collection and processing of personal data in accordance with the applicable Union data protection rules.

As regards data access, the Electricity Directive includes a broad provision under the name of 'data management'. Article 23(1) entitles Member States to specify the eligible parties which may have access to data of the final customer and Article 23(3) requires the processing of personal data carried out within the framework of the Electricity Directive to be in accordance with the GDPR. Article 23(2) states that it is for Member States to organise the management of data 'in order to ensure efficient and secure data access and exchange, as well as data protection and data security'. While the GDPR's RtDP has a specified scope, Member States may thus provide for different and stronger forms of data sharing in the energy sector. At the same time, the scope of the GDPR's RtDP is not limited to a certain class of eligible parties so that data subjects can give their consent to port data to entities not specified by Member States during the implementation of the Electricity Directive. In this regard, one of the requirements imposed on Member States when deploying smart metering systems in Article 20 of the Electricity Directive is to ensure that 'data on the electricity they fed into the grid and their electricity consumption data' is made available to final customers who request it 'through a standardised communication interface or through remote access, or to a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis'.[32] The provision goes on to explain that for these purposes 'it shall be possible for final customers to retrieve their metering data or transmit them to another party at no additional cost and in accordance with their right to data portability under Union data protection rules'. As such, the provision in the Electricity Directive may be understood as an explanation of how the GDPR's RtDP is to be implemented in relation to smart meter data.[33]

In the *automotive sector*, data access is heavily debated as the interests of car manufacturers and third parties in aftersales markets clash.[34] While third-party aftersales service providers claim they need

[32] Article 20(e) Electricity Directive.

[33] For a further discussion of the governance of smart meter data, see Council of European Energy Regulators, 'Review of Current and Future Data Management Models', CEER report, 13 December 2016, < https://www.ceer.eu/documents/104400/-/-/1fbc8e21-2502-c6c8-7017-a6df5652d20b> accessed 8 October 2019; and Netherlands Authority for Consumers and Markets, 'Visie datagovernance energie', 21 March 2019, < https://www.acm.nl/sites/default/files/documents/2019-03/visiedocument-datagovernance-energie.pdf> accessed 8 October 2019.

[34] See also: Bertin Martens & Frank Mueller-Langer, 'Access to digital car data and competition in aftersales services', JRC Digital Economy Working Paper 2018-06, September 2018, <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/access-digital-car-data-and-competition-aftersales-services> accessed 19 April 2019; Wolfgang Kerber & Jonas Severin Frank, 'Data Governance Regimes in the Digital Economy: The Example of Connected Cars', SSRN Working Paper November 2017, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794> accessed 19 April 2019; TRL, Access to In-vehicle Data and Resources, report for the European Commission, May 2017, <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf> accessed 19 April 2019.

access to in-vehicle data in order to provide complementary and innovative services to drivers, car manufacturers argue that there are security and safety risks that make such access undesirable.[35] In May 2018, the European Commission adopted a Communication 'On the road to automated mobility' stating that it would 'consider further options for an enabling framework for vehicle data sharing to enable fair competition in the provision of services in the digital single market, while ensuring compliance with the legislation on the protection of personal data'.[36] While new instruments enabling access to in-vehicle data are anticipated, access to repair and maintenance service information is already regulated. Article 6 of the 2007 Regulation on access to vehicle repair and maintenance information[37] obliges manufacturers to 'provide unrestricted and standardised access to vehicle repair and maintenance information to independent operators through websites using a standardised format'. As such, the Regulation promotes the working of the internal market as clarified in recital 8 stating that unrestricted access to vehicle repair information and effective competition in the market for vehicle repair and maintenance information services are necessary 'to improve the functioning of the internal market, particularly as regards the free movement of goods, freedom of establishment and freedom to provide services'.

In conclusion, this comparison shows that the sector-specific data access regimes are internal market-focused and promote objectives beyond the protection of personal data. In fact, the GDPR can be regarded as a regime that sets the boundaries within which sector-specific data access regimes can regulate other objectives that inevitably relate to the processing of personal data. The references to the GDPR in the sector-specific legislative instruments show that the EU legislator is aware of the parallel application of the different regulatory frameworks. However, the absence of explicit considerations on how the regimes are to be applied alongside each other will create uncertainties in the implementation of such interlinked pieces of legislation as explained below.

2.2 Scope of data and type of control

The scope of the data sharing instrument is key in the level and type of control it confers over the data. As the scope of application is wider and the resulting obligations stronger, the beneficiary will have more control over the data to which it gets access. As a result, the amount or scope of data covered as well as the strength of the available mechanism or type of control determine the effectiveness of a data sharing instrument. In this regard, the regimes do have some important differences in terms of the level and type of control granted over data. At the same time, one should keep in mind that information and power asymmetries in the market can weaken the impact of data sharing tools – irrespective of their strength.

Legislation	Scope of the data	Type of control

[35] See <http://cardatafacts.eu/> accessed 19 April 2019 and ACEA Position Paper, 'Access to vehicle data for third-party services', European Automobile Manufacturers Association, December 2016, available at <https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf> accessed 19 April 2019.

[36] Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 13.

[37] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information [2007] OJ L 171/1.

GDPR	Personal data concerning the data subject and provided to the controller	Copying of data without exclusion from use of data by original controller; no property-like or ownership-like control
Electricity Directive	Metering and consumption data as well as data required for consumer switching	Exact implementation left to the Member States, so that level of control may differ across the EU
PSD2	Access to account needed for a payer to make use of either payment initiation or account information services	Control is purpose-specific, as it specifically relates to the provision of payment initiation and account information services
Regulation on access to vehicle repair and maintenance information	Vehicle repair and maintenance information	Control of technical, non-personal data required for offering repair and maintenance services
Digital Content Directive	Digital content, personal data excluded, provided or created by the consumer when using the digital content or digital service supplied	Retrieval of digital content with an obligation of traders to refrain from continuing to use it; akin to property- or ownership-like control over data

The RtDP of Article 20 GDPR applies to personal data concerning the data subject which he or she has provided to a controller, and where the processing is carried out by automated means and based on consent or a contract.[38] There is still a lot of discussion about the scope of the RtDP, and in particular about the meaning of the term 'provided'. In its Guidelines, the Article 29 Working Party interprets this notion as 'data actively and knowingly provided by the data subject' as well as 'observed data provided by the data subject by virtue of the use of the service or the device'.[39] While 'inferred and derived data' that is created by data controllers on the basis of data 'provided by the data subject' is excluded from the scope, the personal data subject to the RtDP in the view of the Article 29 Working Party also includes a person's search history, traffic and location data, as well as other raw data such as the heartbeat tracked by a wearable device, and generally 'all data observed about the data subject during the activities for the purpose of which the data are collected'.[40] As examples of the latter, the Article 29 Working Party refers to 'transaction history or access log, […] [d]ata collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour)'.[41] Although this broad interpretation is not without criticism,[42] the fact that more data falls within the scope of application of the RtDP in principle means that the level of data control offered to data subjects is stronger – in particular considering the amount of data over which control can be

[38] Article 20(1)(a) and (b) GDPR.
[39] Article 29 Working Party, 'Guidelines on the right to data portability' WP [2017] 242 rev.01, p. 10.; for further discussion see Nikolas Horn & Anne Riechert, 'Practical implementation of the Right to Data Portability', Stiftung Datenschutz 2017, p. 77-81.
[40] Ibid, p. 10.
[41] Ibid, p. 10 footnote 21.
[42] See European Telecommunications Network Operators' Association, 'Legal memorandum with respect to the Article 29 Guidelines on the right to data portability' [2017], p. 3-5, <https://etno.eu/datas/positions-papers/2017/170131%20ETNO_Data%20Portability_Memo/170131%20ETNO_Data%20Portability_Memo.pdf> accessed 19 April 2019.

exercised. An important limit, however, is that once a data subject invokes the RtDP in order to port his or her personal data to a new controller, this does not automatically trigger an obligation on the original controller to delete the ported data. The right of erasure of Article 17 GDPR can be invoked in parallel, but has a more limited scope than the RtDP. As such, the RtDP involves copying of data and does not exclude the original controller from continuing to process the personal data that is transferred. Because of the absence of a right to exclude, the nature of control granted to data subjects with the RtDP does not equal a property-like or ownership-like control.[43]

In the *energy sector*, Article 23(1) of the Electricity Directive states that for the purposes of the Directive data includes 'metering and consumption data as well as data required for customer switching, demand response and other services'. This data would at least partly concern personal data as it relates to a customer's energy profile (the Directive does not make explicit whether other data, for instance raw energy data, would also be included), so that there is an overlap with the GDPR's RtDP. In order to get access to this data, the eligible party (to be specified by the Member State, as explained in the next section) must have the explicit consent of the final customer.[44] As regards the level of control, it is worth pointing out that the Electricity Directive leaves the exact implementation of Article 23 to the Member States who have to ensure 'easy' and 'efficient and secure data access and exchange'.[45] What may seem like slight differences in the way in which the data management models are adopted by the Member States (for instance whether data access is limited to certain purposes to be facilitated on the basis of the data), can impact the level of control over data as the procedures chosen are key in this regard.[46] It is therefore desirable from an internal market perspective to ensure common approaches among Member States in implementing the provision as much as possible.

In the *payment sector*, the scope of the access-to-account rule is limited to what is needed for a payer to make use of either payment initiation or account information services upon the payer's explicit consent.[47] The provision of these services implies the processing of the payer's financial information, which qualifies as personal data under the GDPR if the payer is a natural person. A key difference between the GDPR's RtDP and the PSD2's access-to-account rule is that the latter only applies to the two services specified, whereas the former is a general-purpose regime that applies irrespective of the future use of the personal data that is ported.[48] Because of the wider scope, one can argue that the level of control granted by the RtDP is higher than that provided under the PSD2 – at least considering the reach of situations covered.

In the *automotive sector*, Article 3(14) of the Regulation on access to vehicle repair and maintenance information the term 'vehicle repair and maintenance information' is defined as 'all information

[43] See the analysis in Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1368.
[44] Article 23(1) and (2) Electricity Directive.
[45] Article 23(2) Electricity Directive.
[46] For a discussion of the uncertainty left by the provisions of the Electricity Directive for regulating data access, see Charlotte Ducuing, 'Mandating Data Sharing to Establish Data as an Infrastructural Resource' (2019) 21 *Network Industries Quarterly* 21, 23-24.
[47] Article 66(2) and 67(2)(a) PSD2.
[48] See also Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1369. The authors argue that the GDPR's RtDP 'does not confine the exercise of the control with some types of socially beneficial activity or social goals. In this sense, it is completely "purpose agnostic"'.

required for diagnosis, servicing, inspection, periodic monitoring, repair, re-programming or re-initialising of the vehicle and which the manufacturers provide for their authorised dealers and repairers' and 'includes all information required for fitting parts or equipment on vehicles'.[49] While this constitutes technical, non-personal data, the discussions about access to in-vehicle data beyond repair and maintenance information do concern personal data.[50] Information from the vehicle may identify a natural person based on for instance driving patterns or through combining it with other datasets.[51] In this regard, the Commission stated in its Communication 'On the road to automated mobility' that there is a need to strike 'a balance between fair competition, the possibility for consumer to have access to different services, safety, cybersecurity, *in full compliance with the legislation on competition* and *on the protection of personal data such as user consent for data sharing*' (emphasis added).[52] While the exact scope of a data sharing remedy for in-vehicle data thus still needs to be determined, it is clear that the Commission aims to take into account competition and data protection considerations.

As regards *digital content/services*, the data retrieval obligation of Article 16(4) of the Digital Content Directive relates to 'any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader'.[53] By excluding personal data from the scope of the data retrieval obligation, the legislator has tried to avoid any overlap with the GDPR's RtDP.[54] As such, the two regulatory instruments can complement each other – although one may wonder whether it is possible to distinguish personal and non-personal data from one another as datasets will often be mixed.[55] In terms of the level of control, the data retrieval obligation is stronger than the RtDP considering that the Digital Content Directive obliges the supplier to refrain from using any content other than personal data which was provided or created by the consumer when using the digital content or digital service, except where the content 'has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content'.[56] Such an obligation of traders to refrain from continuing to use digital content is akin to property- or ownership-like control over data.[57] At the same time, the data retrieval obligation is not without limits. In particular, the trader is not required to make digital content available where such content: (a) 'has no

[49] Article 6(2) of the Regulation on access to vehicle repair and maintenance information lists in sub (a) to (i) in more technical terms the information subject to the access obligation of manufacturers.

[50] Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle' (2018) 9 *JIPITEC* 310, 323-324 and 326-327.

[51] Zang Hui and Jean Bolot, 'Anonymization Of Location Data Does Not Work: A Large-Scale Measurement Study', in Proc. of MobiCom 11 (2011).

[52] Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 12-13.

[53] Article 2(1) of the Digital Content Directive defines 'digital content' as 'data which are produced and supplied in digital form'.

[54] This was different in the Commission proposal for a Digital Content Directive where personal data was not excluded and Article 13(2)(c) obliged the supplier to 'provide the consumer with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent that data has been retained by the supplier'. For a comparison between the GDPR's RtDP and the data retrieval obligation in the Digital Content Directive, see Axel Metzger, Zohar Efroni, Lena Mischau & Jakob Metzger, 'Data-Related Aspects of the Digital Content Directive' (2018) 9 *JIPITEC* 90, 102-105.

[55] See Inge Graef, Raphaël Gellert & Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (2019) 44 *European Law Review* 605, 610-611.

[56] Article 16(3)(d) of the Digital Content Directive.

[57] See Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1393.

utility outside the context of the digital content or digital service supplied by the trader'; (b) 'only relates to the consumer's activity when using the digital content or digital service supplied by the trader'; and (c) 'has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts'.[58]

2.3 Beneficiaries

In terms of the parties entitled to data access, the regulatory frameworks are quite straightforward and clearly differ from one another.

Legislation	**Beneficiary**
GDPR	Data subjects (natural persons)
Digital Content Directive	Consumers (natural persons)
Regulation on access to vehicle repair and maintenance information	Independent operators of repair and maintenance services for motor vehicles
PSD2	Third-party payment initiation and account information service providers, payers
Electricity Directive	Final customers; eligible parties to be specified by the Member States

The *GDPR* provides data subjects with the RtDP. Article 4(1) GDPR defines a 'data subject' as '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'.

The *Digital Content Directive* also applies to individuals as beneficiaries of the data retrieval obligation, and more in particular to a 'consumer' defined in Article 2(6) as 'any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession'.

Article 6(1) of the *Regulation on access to vehicle repair and maintenance information* explicitly mentions independent operators as the beneficiaries of data access. Article 3(15) defines 'independent operators' as 'undertakings other than authorised dealers and repairers which are directly or indirectly involved in the repair and maintenance of motor vehicles'.

Similarly, Articles 66 and 67 of the *PSD2* provide payers with the right to make use of payment initiation and account information services.[59] In practice, it will rather be the third party service providers who invoke the access-to-account rule vis-à-vis banks in order to offer their services to payers. Recital 93 confirms this by stating that the adoption of common and open standards should ensure that the bank 'is aware that he is being contacted by a payment initiation service provider or an account information service provider and not by the client itself'. However, strictly speaking payers are the direct

[58] Article 16(3)(a)(b)(c) of the Digital Content Directive.

[59] According to Article 4(8) of the Digital Content Directive, a payer is 'a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order'.

beneficiaries of the access-to-account rule of the PSD2. In this regard, Articles 66(1) and 67(1) state that 'Member States shall ensure that a payment service user has the right to make use of' either payment initiation and account information services.[60] Although the access-to-account rule is thus phrased as a right of payers, the data access that it enables will be configured and implemented by the third party service providers. As a result, it is important that payers are adequately informed by third parties about what exact forms of data access they consent to.

The *Electricity Directive* provides the least clarity in terms of beneficiaries as it leaves the specification of the 'eligible parties' up to the Member States. Article 23(1) states that Member States have to 'specify the rules on the access to data of the final customer by eligible parties'. This implies that there can be differences across the European Union as to how data sharing in the energy sector is implemented, which would not be a welcome development from an internal market perspective. Another interesting point is that the Electricity Directive seems to configure data access both as a right or entitlement of individuals and as an entitlement of eligible businesses. This distinguishes the approach in the energy sector from the one in the PSD2, which instead grants payers the right to use payment initiation and account information services but configures it as a form of data access between banks and the third parties offering the services.

Beyond the direct beneficiaries who can invoke the regulatory instruments, there are of course *indirect beneficiaries* as well. The GDPR's RtDP applies to data subjects, but also indirectly benefits data controllers who may incentivise individuals to bring their personal data with them when switching services. Similarly, individuals can be considered indirect beneficiaries of the regimes in the automotive and energy sectors because of the wider choice of complementary services that is enabled by the parties that invoke the data access tools. This means that the impact of the regimes go beyond the beneficiaries who can invoke the data access instruments. At a higher socio-economic level, the different regimes also further more abstract goals that benefit the internal market, data protection, consumer empowerment, etc. as discussed in section 2.1 above.

2.4 Configuration

Apart from the scope of data and the beneficiaries, the further configuration of the data sharing tools is key in determining their impact because the implementation in practice will depend on how the legislator configured the respective instruments. As discussed in this section, each of the regimes has a different way of operating in this regard.

Legislation	**Configuration**
GDPR	Between controllers and data subjects
Regulation on access to vehicle repair and maintenance information	Between car manufacturers and independent operators of repair and maintenance services
Electricity Directive	Between electricity undertakings and final customers; and between electricity undertakings

[60] Article 4(15) PSD2 defines a 'payment initiation service' as 'a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service'. As regards the definition of 'account information service', Article 4(16) refers to 'an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider'.

	and eligible parties specified by individual Member States
PSD2	Between banks,[61] and third-party payment initiation and account information service providers
Digital Content Directive	Between traders and consumers

Since both of them provide entitlements to individuals, the *GDPR* and the *Digital Content Directive* are configured via the user who invokes the RtDP or the data retrieval mechanism in order to have data transferred to a new provider. The Digital Content Directive only entitles consumers to have digital content retrieved and not to have it transferred as well. However, the fact that suppliers have to make the digital content available 'in a commonly used and machine-readable format'[62] does indicate that the underlying idea is to give consumers the possibility to reuse the content in other services. The data retrieval obligation is only triggered in situations of contract termination, which may explain why its configuration does not include direct transfer of digital content between suppliers.[63] However, one can argue that it would nevertheless be desirable to facilitate such direct transfers in case consumers wish to switch to a new supplier after terminating an existing contract.

The configuration of the GDPR's RtDP consists of two elements in this regard: (1) a right of data subjects to receive their personal data provided to a controller, combined with a right to transmit those data to another controller;[64] and (2) a right of data subjects to have the personal data directly transmitted from one controller to another where technically feasible.[65] In the first case, the data subject has to save and store the data from controller A him- or herself and subsequently make sure to upload/submit it to controller B. In the second case, the data subject simply files the request and the controllers take care of the transfer among themselves. The question, however, is when such direct transfer is to be regarded as 'technically feasible' within the meaning of Article 20(2) GDPR.

The data access tools in the *automotive*, *energy* and *payment* sectors are all configured as leading to direct transfers between businesses.[66] In the automotive sector, this is most clear as the data covered in the Regulation on access to vehicle repair and maintenance information does not concern personal data and is exchanged between car manufacturers and independent operators. This will be different when new forms of access to in-vehicle data are devised that do relate to natural persons, as hinted at by the Commission in its May 2018 Communication 'On the road to automated mobility' that is discussed above.[67]. In that case, the role of the driver must be considered when data is transferred from car manufacturers to third-party aftersales service providers. In the payment sector, the interests of the

[61] The term used by the PSD2 is 'account servicing payment service provider' defined by Article 4(17) PSD2 as 'a payment service provider providing and maintaining a payment account for a payer'.
[62] Article 16(4) of the Digital Content Directive.
[63] See Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1393.
[64] Article 20(1) of the GDPR.
[65] Article 20(2) of the GDPR.
[66] Please note that Article 20(e) of the Electricity Directive also foresees data access to take place between electricity undertakings and final customers as a type of data portability.
[67] Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 13.

individual are protected by requiring the third parties at stake to obtain explicit consent from the relevant customer to access data. Articles 66(2) and 67(2)(a) PSD2 simply refer to 'explicit consent' without specifying the applicability of the GDPR. As regards the energy sector, Article 23(3) of the Electricity Directive requires the processing of data carried out for the purposes of the Directive to take place in compliance with the GDPR, without referring to the notion of explicit consent. A relevant question is whether this implies that data sharing under the Electricity Directive may also take place on the basis of another ground of processing, such as a contract, legal obligation or legitimate interest of the controller which would not require the involvement of a data subject.

Apart from the direct transfer of data between businesses, there is another factor that distinguishes the GDPR's RtDP and the data retrieval obligation in the Digital Content Directive from the data access regimes in the energy, payment and automotive sectors. The latter give rise to a continuous stream of data, as long as the individual does not withdraw his or her consent. For instance, continuous and real-time access to data is required for providing services that track a customer's energy consumption or for offering services that bring account information from different payment accounts together in one application. The GDPR's RtDP and the data retrieval obligation of the Digital Content Directive seem, however, envisaged for a more static setting where a data subject/consumer files a request to the data controller/supplier as a one-off mechanism. Once the data is ported/retrieved, there are no further data streams. This is an important difference, as it has consequences for the relationship between the different regimes as further discussed in section 3 below.

2.5 Modalities

The conditions under which data access is provided, such as the applicable costs and time limits, are a further factor determining the scope of the respective instruments. Interestingly, there is some convergence in the modalities of data sharing as laid down in the different regimes.

Legislation	**Modalities**
GDPR	Free of charge/reasonable fee, without undue delay (within one month)
Digital Content Directive	Free of charge, without hindrance from the trader, within a reasonable time
Electricity Directive	Free of charge to final customers, but fees for eligible parties to be set by individual Member States
Regulation on access to vehicle repair and maintenance information	Reasonable and proportionate fees, non-discriminatory compared to authorised dealers and repairers, availability of information on a daily, monthly, and yearly basis
PSD2	Obligation not to discriminate against payment initiation and account information service providers, other than for objective reasons

Article 12(5) of the *GDPR* states that actions taken to comply with data subject requests more generally, including the RtDP have to be provided free of charge. However, if data subject request are 'manifestly

unfounded or excessive, in particular because of their repetitive character', the controller may either charge 'a reasonable fee taking into account the administrative costs' or refuse to act. Article 12(3) of the GDPR requires controllers to provide information on action on data subject requests 'without undue delay and in any event within one month of receipt of the request'. This period may be extended by two additional months 'where necessary, taking into account the complexity and number of the requests'.

As regards *digital content/services*, Article 16(4) of the Digital Content Directive entitles consumers to retrieve digital content 'free of charge, without hindrance from the trader, within a reasonable time'. Recital 71 clarifies that an exception to the free of charge retrieval of digital content are 'costs generated by the consumer's own digital environment, for instance the costs of a network connection as those costs are not specifically linked to the retrieval of the content'. The terms 'without hindrance' and 'reasonable time' are not further specified. In the *energy* sector, Article 23(5) of the Electricity Directive states that no additional costs may be charged to final customers for access to their data or for a requests to make their data available. It is up to Member States to establish the relevant charges for eligible parties to access data. A limit that the provision sets is that Member States have to ensure that 'any charges imposed by regulated entities that provide data services are reasonable and duly justified'. The Electricity Directive does not specify the applicable time limits. Article 23(2) only states that Member States have to ensure 'efficient and secure data access and exchange' and that eligible parties should have the requested data 'at their disposal in a non-discriminatory manner and simultaneously'.

Article 7 of the Regulation on access to vehicle repair and maintenance information provides detailed rules under which car manufacturers have to provide access to independent operators in the *automotive sector*. Article 7(1) entitles manufactures to charge 'reasonable and proportionate fees'. The provision continues by specifying that a fee is not reasonable or proportionate 'if it discourages access by failing to take into account the extent to which the independent operator uses it'. In addition, manufacturers must offer access to the vehicle repair and maintenance information 'in a manner which is non-discriminatory compared to the provision given or access granted to authorised dealers and repairers'.[68] In relation to the timing, Article 7(2) makes clear that manufactures have to make vehicle repair and maintenance information available 'on a daily, monthly, and yearly basis, with fees for access to such information varying in accordance with the respective periods of time for which access is granted'.[69]

The modalities of data sharing are the least specified for the *payment* sector. Articles 66(4)(c) and 67(3)(b) of the PSD2 mainly require banks to treat payment orders and data requests transmitted through the services of a third party provider 'without any discrimination other than for objective reasons'. Recital 50 explains that any payment service provider competing in the internal market should be able 'to use the services of the technical infrastructures of those payment systems under the same conditions' and that differences in price conditions should only be allowed 'where that is motivated by differences in costs incurred by the payment service providers'. With regard to payment initiation services, Article 66(4)(c) further specifies that the notion of non-discrimination applies 'in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer'. Whether

[68] Article 7(1) of the Regulation on Access to Vehicle Repair and Maintenance Information.

[69] Articles 13 and 14 of Regulation 2017/1154, supplementing Regulation (EC) No 715/2007 [2017] OJ L 175/1 provide additional details in terms of compliance with access to vehicle repair and maintenance information, but do not change the right of manufacturers to impose an access fee.

a bank is allowed to charge fees to third party providers for making use of the access-to-account rule thus depends on whether it charges fees for payment orders and data requests beyond those facilitated by payment initiation and account information service providers.

2.6 Standardisation

When it comes to the implementation of the data sharing instruments in practice, the availability of technical standards is key in order to ensure that data can be effectively exchanged between businesses. While some regimes explicitly commission the development of standards to an authority, others simply refer to the desirability of standards to evolve with specifying any procedure to be followed.

Legislation	**Standardisation**
GDPR	Structured, commonly used and machine-readable format – data controllers are encouraged to develop interoperable formats
Digital Content Directive	Commonly used and machine-readable format
Electricity Directive	Common data format at national and later EU level
Regulation on access to vehicle repair and maintenance information	Websites using a standardised format in a readily accessible manner
PSD2	European Banking Authority specifies the requirements of common and open standards

The *Digital Content Directive* requires suppliers to make digital content available to consumers 'in a commonly used and machine-readable format'.[70] Recital 50 requires traders to make use of 'standards, open technical specifications, good practices and codes of conduct […] whether established at international level, Union level or at the level of a specific industry sector'. In addition, the recital states that 'the Commission could call for the development of international and Union standards and the drawing up of a code of conduct by trade associations and other representative organisations that could support the uniform implementation of this Directive'. These statements are still fairly open in terms of the type and scope of action, but do illustrate that standardisation is seen as a factor for the success of the Digital Content Directive.

In this context, it is interesting to note that the statements about standardisation in the Commission's original proposal for the *GDPR* were also scaled down in the final version. Article 18(3) of the Commission's proposal for the GDPR provided the Commission with the possibility to specify 'the technical standards, modalities and procedures for the transmission of personal data'.[71] In its final version, recital 68 of the GDPR merely provides that '[d]ata controllers should be encouraged to develop interoperable formats that enable data portability'. At the same time, the RtDP 'should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible'. The Article 29 Working Party concludes from this statement that 'portability aims to produce

[70] Article 16(4) of the Digital Content Directive.

[71] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM/2012/011 final.

interoperable systems, not compatible systems'.[72] In the view of the Article 29 Working Party, the terms 'structured', 'commonly used' and 'machine-readable' are a set of 'minimal requirements that should facilitate the interoperability of the data format provided by the data controller' and as such are 'specifications for the means, whereas interoperability is the desired outcome'.[73] Although the GDPR applies horizontally across the entire economy, the Article 29 Working Party argues that the 'most appropriate format will differ across sectors'.[74] A sector-specific approach to establishing the 'structured, commonly used and machine-readable format' through which to port the data seems therefore the preferred approach. This leads to interesting spill-overs with the sector-specific data access regimes as discussed below in section 3.

The *energy* sector is instructive in this regard, as Article 24(2) of the Electricity Directive specifically requires the Commission to adopt 'interoperability requirements and non-discriminatory and transparent procedures for access to data' by means of implementing acts. It is then up to Member States to ensure that electricity undertakings apply those interoperability requirements and procedures for data access.[75] In particular, Article 24(3) states that those requirements and procedures have to 'be based on existing national practices'. And Article 24(1) imposes the responsibility to facilitate 'full interoperability of energy services' in the EU on Member States as a way 'to promote competition in the retail market and to avoid excessive administrative costs for the eligible parties'. Once the Commission has adopted the interoperability requirements and procedures for data access, market participants will thus be able to use common approaches across electricity markets within the entire EU so to stimulate the internal market.

As for the *automotive* industry, Article 6(1) of the Regulation on access to vehicle repair and maintenance information requires manufactures to provide 'unrestricted and standardised access […] through websites using a standardised format in a readily accessible and prompt manner'. To facilitate the achievement of this objective, it is required for the information to be submitted 'in a consistent manner', in accordance with the technical requirements of the so-called OASIS format.[76] Beyond the remit of vehicle repair and maintenance information for which a standard and procedure thus already exists, the current discussions in the automotive sector concern the way in which real-time access to in-vehicle data is to be provided. There are three main technical solutions envisaged: access through (a) a data server platform; (b) an in-vehicle interface; and (c) an on-board application platform.[77] Each of these options has its advantages and disadvantages on either accessibility, competition or reliability. Car

[72] Article 29 Working Party, 'Guidelines on the right to data portability' WP [2017] 242 rev.01, p. 17.
[73] Ibid, p. 17.
[74] Ibid, p. 17.
[75] Article 24(3) Electricity Directive.
[76] Footnote 23 of the Regulation on Access to Vehicle Repair and Maintenance Information specifies that: '[T]he 'OASIS format' refers to the technical specifications of OASIS Document SC2-D5, Format of Automotive Repair Information, version 1.0, 28 May 2003 (<http://www.oasis-open.org/committees/download.php/2412/Draft%20Committee%20Specification.pdf> accessed 19 April 2019) and of Sections 3.2, 3.5, 3.6, 3.7 and 3.8 of OASIS Document SC1-D2, Autorepair Requirements Specification, version 6.1, dated 10.1.2003 (<http://lists.oasis-open.org/archives/autorepair/200302/pdf00005.pdf> accessed 19 April 2019), using only open text and graphic formats'.
[77] TRL, 'Access to In-vehicle Data and Resources' [May, 2017] Report for the European Commission, p. 6 <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf> accessed 19 April 2019.

manufacturers prefer the use of a data server platform such as the Extended Vehicle concept. However, this may not be desirable from the perspective of the welfare of drivers and aftersales service providers as the concept implies that all car data would be collected exclusively on data servers ran by the car manufacturer.[78] There is thus a need to find an approach adequately reconciling the different interests of stakeholders in the automotive sector, namely car manufacturers, aftersales service providers and drivers.

Standardisation is a crucial element for the success of the PSD2 in the *payment* sector. For implementing access-to-account, the European Banking Authority adopted several Guidelines and Regulatory Technical Standards to clarify the steps banks need to take, and several initiatives are defining common standards for Application Programming Interfaces (APIs).[79] In accordance with recital 93 of the PSD2, 'open standards should ensure the interoperability of different technological communication solutions'. The protection of personal data also plays a role in the development of regulatory technical standards on authentication and communication. Recital 94 namely requires the European Banking Authority to 'systematically assess and take into account the privacy dimension, in order to identify the risks associated with each of the technical options available and the remedies that could be put in place to minimise threats to data protection'. A concern about the success of the access-to-account rule in the PSD2 is that several parallel standards will develop, so that the level of interoperability and harmonisation across the EU is limited.[80] The so-called 'Berlin Group', involving several stakeholders in the payment sector, is working on the development of an open, common and harmonised European API standard.[81]

As a result, there are several initiatives relating to standardisation in the different sectors by market players as well as regulatory authorities.[82] These standards that are being developed for the respective sectors may also facilitate the further implementation of the GDPR's RtDP. This is one example of the spill-overs discussed in the next section.

3. Analysis of interactions and spill-overs

The above comparison of the various data sharing regimes illustrates the difference in scope of the resulting actions. Despite their distinct scope, interactions will arise between the GDPR's RtDP and sector-specific regimes because each of them results into entitlements to access personal data. The fact

[78] Bertin Martens & Frank Mueller-Langer, 'Access to digital car data and competition in aftersales services' (2018) JRC Digital Economy Working Paper 2018-06, p. 4-5.

[79] For a discussion, see Giuseppe Colangelo & Oscar Borgogno, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule' (2018) *EU Law Working Papers No. 35, Stanford-Vienna Transatlantic Technology Law Forum*, p. 22-27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251584> accessed 19 April 2019.

[80] Markos Zachariadis & Pinar Ozcan, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking', *SWIFT Institute Working Paper No. 2016-001* (2017), p. 23.

[81] Giuseppe Colangelo & Oscar Borgogno, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule' (2018) *EU Law Working Papers No. 35, Stanford-Vienna Transatlantic Technology Law Forum*, p. 25 footnote 75.

[82] For an analysis of how APIs are used as a tool to implement data sharing across sectors, see Oscar Borgogno & Giuseppe Colangelo, 'Data sharing and interoperability: Fostering innovation and competition through APIs' (2019) 35 *Computer Law & Security Review* 1.

that such overlap exists is not problematic in and of itself. Because each regime furthers its own objective, there may be a welcome complementarity in terms of the type and scope of the various actions. However, where data sharing regimes overlap their interaction will inevitably lead to questions about how to interpret and implement their respective requirements. We theorise that the presence of sector-specific and horizontal regimes will lead to a set of spill-overs, which we define as an unintended impact of the substance of the rules of one area on the other. Such spill-overs can be merely *factual* (e.g. over-compliance by firms to save costs of a fragmented landscape) or *legal* (e.g. expansion of regimes due to changing interpretation of open norms). This impact can be bi-directional, that is from horizontal regimes to sectorial regimes and from sectorial regimes to horizontal regimes. We anticipate more spill-overs in the direction of horizontal regimes. We posit that such effects may even help to overcome the current piecemeal approach of regulating data sharing in the EU and eventually lead to a more horizontal, overarching framework. At the same time, tensions may emerge where regimes have distinct requirements in place. Hence such spill-overs should not be immediately equated with positive effects on society. To demonstrate this, we identify the following main examples of anticipated spill-over effects: (1) complementarity/substitution, (2) one-off/continuous access, (3) expansion through open norms, and (4) price of access/use of data.

3.1 Data sharing for complementarity, substitution, or both?

Unlike the GDPR's RtDP, the sector-specific regimes discussed above do not relate to the portability of data as such.[83] Instead, these regimes provide entitlements to access data. However, both data portability and data access lead to empowerment of individuals and/or businesses in a situation of dependence on a third party to use data.[84] In our view, these policy interventions differ, among other things, by the goals they pursue. While the data access policies aim to incentivise data sharing for complementary services, the portability policies aim to incentivise complementary and substitute services at the same time because they do not limit the purpose of the use of data.

In the case of *access*, the data remains with the original provider/controller that will act as the intermediary between the party invoking data access and the new data controller. Data access is therefore particularly suitable for *complementary services* that require continuous access to real-time data and build upon the infrastructure provided by the original provider/controller. The access-to-account rule of the PSD2 is a good example. Upon consent of the payer, third-party providers will have access to the latter's payment account in order to initiate payment transactions via an internet application or to consolidate account information from one or more accounts into one application.[85] Real-time access is needed for such services, as a result of which the bank remains in place as the intermediary providing the infrastructure for the complementary services.

[83] Here it is worth referring to the Regulation on the free flow of non-personal data which does include a portability tool beyond the GDPR, namely for the porting of non-personal data between cloud service providers in business-to-business relations. Article 6 of Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 empowers the Commission to encourage and facilitate the development of self-regulatory codes of conduct, including 'best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format'.

[84] Nikolas Horn & Anne Riechert, 'Practical implementation of the Right to Data Portability', Stiftung Datenschutz 2017, p. 74.

[85] See Articles 66 and 67 of the PSD2.

Data portability, in turn, is fit for situations where third parties need a copy of the data from the original provider/controller to be able to develop their own services. Unlike in cases of data access, data portability results into the physical copying[86] of datasets to the new provider/controller without the need for continued reliance on the original provider/controller. As such, data portability is especially apt to facilitate the development of *substitutes or complements* that only require a one-off (as opposed to data access that is continuous) copying of data that is then further processed by the new provider/controller. An example of the former is the porting of one's social network profile to a substitute platform that competes with the original provider/controller, for instance from Facebook to Google+. As regards a complementary service that requires one-off portability, one can think of the porting of one's contacts in a social network to an application that draws up an address book with the contact details of one's connections from several platforms. Once the data is ported/copied to the application, the new provider/controller will further process the data for the individual without having to rely on the infrastructure provided by the original social network provider.

When sectorial data access policies and horizontal portability policies interact, they might result in spill-overs under which an infrastructure developed for complementary services, such as standards or APIs, is eventually relied upon for substitute services through horizontal regimes like the GDPR's RtDP. This means that a horizontal policy that applies irrespective of the purpose could be broadened in its reach due to technological developments which were initially developed for closed-use scenarios of data access.

This carries with itself as a risk too. Data portability generally implies higher security risks involved in actual data transfers to third parties. Data access policies, on the other hand, appear to generally allow the original providers to regulate individual access by technical means since the data does not necessarily leave their platform. The level of control given to beneficiaries thus seems correlated with risks associated with the data that is being shared. The greater the control, the greater the risk and thus the responsibility for follow-on use of the data. Such differences illustrate the different focus of the GDPR's RtDP and the sector-specific data access regimes.

3.2 Continuous versus one-off data sharing

Another example of a spill-over effects resulting from the interaction between the GDPR's RtDP and the sector-specific data access regimes concerns the question of whether the instruments facilitate continuous or only one-off data sharing. The provision of dynamic and real-time services, which will gain in importance as illustrated by the configuration of the sector-specific regimes in the energy, payment and automotive sectors discussed in section 2.4, require continuous access to data.

The legislative history illustrates that the GDPR's RtDP was mainly envisaged to apply as a one-off mechanism to stimulate direct competition. In its 2012 Impact Assessment, the Commission refers to social networks by way of example.[87] However, as made clear by the European Data Protection

[86] Since the GDPR's RtDP does not automatically entail deletion of the ported data, it is more accurate to speak of copying rather than transfer of data.

[87] Commission 'Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)' (Staff Working Paper) SEC (2012) 72 final, p. 106 ('[t]he possibility

Supervisor in 2014, the RtDP can also enable individuals to take advantage of value-added services offered by third parties.[88] By letting an individual port personal data from the original service to a complementary service, the RtDP stimulates follow-on innovation and indirect competition as well. However, where such complementary services build upon the functionality provided by the original service, a form of continuous, real-time access may instead be required as discussed in the previous section in the context of the PSD2. Real-time access to one's payment account is required in order for third parties to initiate payment transactions or to consolidate account information. Another example is smart driving where one could envisage an application that alerts the driver once the car runs out of fuel. Based on the location of the car, the service could then direct the driver to a nearby petrol station that is part of its network and possibly even provide a discount. In such circumstances, there has to be a continuous stream of real-time data between the application and the car. Reliance on the car infrastructure is essential for the application to function, so that a one-off portability is not satisfactory.[89] Despite the fact that such uses strengthen the control of individuals over their personal data and thus fit with the rationale behind the RtDP, there are several indications in the GDPR that such a continuous form of access was not envisaged by the EU legislator under Article 20. In other words, it does not count among the original goals of the instrument. This implies that other regulatory measures are needed to facilitate continuous data sharing in specific sectors.

Other provisions of GDPR seem to confirm this. Article 12 GDPR lays down the modalities for the exercise of the rights of data subjects, including the RtDP. With regard to the time period within which the data controller has to comply with requests from data subjects, Article 12(3) GDPR states that the controller has to provide the data subject with information on the action taken 'without undue delay and in any event within one month of receipt of the request'. An extension of two additional months may apply 'where necessary, taking into account the complexity and number of the requests'. Such time limits do not fit with a dynamic environment like smart driving where an effective experience for drivers and/or data subjects requires a seamless and continuous transfer of data. Article 12(5) GDPR even allows controllers to reject requests that are 'manifestly unfounded or excessive, in particular because of their repetitive character'.

One may thus wonder to what extent the GDPR's RtDP, and the rights of data subjects more generally, can ever be regarded as one-off mechanisms. Even if in the example of smart driving it would be technically possible to comply immediately with a data portability request every time the driver/data subject gets into his or her car for a new drive[90] (so that the normal time limit of one month would not

---

to move data from one service provider to another would increase competition in some sectors, e.g. between social networks, and could also make data protection an element in this competition, when users decide to move away from a service they do not consider appropriate in terms of data protection').

[88] European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (Preliminary Opinion) [2014], para 26.

[89] Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle' (2018) 9 *JIPITEC* 310, 326-327.

[90] Irrespective of its scope, such an application of data portability or data access would in any case be needed to comply with the GDPR since a car can be used by multiple individuals (even if it is registered only on one person's name). An authentication mechanism to identify the data subject each time he or she enters the car would therefore

apply), it remains to be seen to what extent such a use of Article 20 GDPR's RtDP can be considered excessive because of its 'repetitive character'. If so, the car manufacturer may charge an administrative fee or even refuse to comply with the request altogether. In its Guidelines on data portability, the Article 29 Working Party did indicate that the availability of automated systems, such as APIs in the case of information society services, can lessen the potential burden resulting from repetitive requests. As a consequence, in the view of the Article 29 Working Party 'there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests'.[91] While such an interpretation might be welcomed from the perspective of the effectiveness of the GDPR's RtDP, the guidelines of the Article 29 Working Party are not legally binding and in fact set aside the option included by the EU legislator for a data controller to refuse to comply with a data portability request. As such, one can argue that the Article 29 Working Party is proposing an interpretation that seemingly contradicts Article 20 GDPR so that the CJEU may reinstate the possibility of a data controller to refuse compliance where data portability requests are considered excessive. Because of these uncertainties in the interpretation of the GDPR, the current efforts of the Commission to explore and develop other measures for facilitating continuous, real-time access to in-vehicle data in the automotive sector, in line with what the PSD2 has done for the payment sector, are to be welcomed.[92]

At the same time, it remains open to what extent the development of sectorial data access policies can be stopped from having spill-over effects on horizontal data portability regimes. If the infrastructure for continuous access is put at place, albeit for a different purpose, it might be hard to put the genie back to the bottle for the concerned industry. Despite original intentions of the legislators, it would take a real self-restraint by the authorities and judges to resist the temptation to use the same real-time infrastructure for compliance with data portability requests. Considering the dynamic nature of current services, the possibility to establish a continuous and real-time stream of data between providers might be often desirable. This would require the development of adequate standards and processes, either at the initiative by the market players, governed by the legislator or a regulatory authority, or a combination thereof. While this involves serious effort by all relevant stakeholders, such an outcome does not seem unfeasible when observing the ongoing developments in the energy, payment and automotive sectors regarding standardisation. In the context of access to public sector data, the new Open Data and Public Sector Information Directive, which was adopted in June 2019, provides more possibilities for real-time access to dynamic data.[93] Similarly, direct transfers between providers are more effective than a form of portability or retrieval of data where an individual has to extract information him- or herself and then upload it again to a new provider. As a result, a broad

be necessary to prevent that the data transfer takes place without the consent of the individual whose movements are being tracked.

[91] Article 29 Working Party, 'Guidelines on the right to data portability' WP [2017] 242 rev.01, p. 15.

[92] See Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 13. For a discussion on the welfare effects from an economic perspective, see Bertin Martens & Frank Mueller-Langer, 'Access to digital car data and competition in aftersales services' (2018) JRC Digital Economy Working Paper 2018-06, p. 19.

[93] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56.

interpretation of 'technical feasibility' in Article 20(2) GDPR, so that data subjects will have a right to ask for their personal data to be ported among data controllers, might be irresistible.

3.3 Expansion of data sharing through open norms

GDPR's RtDP instrument is designed with a number of *open norms*, such as 'personal data', 'technical feasibility' and 'undue delay', which predetermine its scope. As some sectorial data access regimes prescribe the technical infrastructure for their own regimes, they make it de facto available also for more horizontal instruments. The question remains whether these open norms will absorb availability of such infrastructure, thus raising the bar, or simply ignore it. In its Guidelines on data portability, the Article 29 Working Party states that where regimes other than the GDPR also provide for some form of portability of the data concerned 'the conditions laid down in these *specific laws* must also be taken into account when satisfying a data portability request under the GDPR'.[94]

With the rise of the Internet of Things, the number of situations in which the GDPR's RtDP can become of use are only going to grow. Because of the ever-expanding notion of '*personal data*',[95] more and more information gathered by devices in our homes will fall within the reach of the GDPR as long as they can be traced back to an individual.[96] With more information becoming personal data, the scope of application of the GDPR's RtDP expands as well. As a result, where sector-specific regimes are present, their interaction with the GDPR's RtDP will gain in importance. In this regard, it will be interesting to see how industry-specific developments are going to impact the interpretation and implementation of Article 20 GDPR. For instance, the PSD2 and the Electricity Directive are leading to the development of standards to facilitate data access. Such standardisation of data formats and interoperability between systems also increase the '*technical feasibility*' of direct transfers of personal data under Article 20 GDPR. In our view, it is likely that the presence of sector-specific interventions will help to interpret such open norms in the scope of the GDPR's RtDP. Similarly, the term '*without undue delay'* in Article 12(3) GDPR for compliance with a data subject's request for data portability can hardly be interpreted as a period of one month if a sector-specific regime enables instantaneous access to data. The same can be said of the room for data controllers to refuse to act when requests for data portability are 'manifestly unfounded or excessive, in particular because of their repetitive character'. Where sector-specific regimes provide for continuous access to data (such as the PSD2 and the Electricity Directive), it will in our view be hard to interpret Article 20 GDPR without reference to conditions and frameworks created by sectorial access regimes. The openness of the relevant notions in Article 20 GDPR provides sufficient room for this. Irrespective of whether enforcement actions by data protection authorities or judgments from the EU courts will require such proactive approaches, spill-overs are likely to occur already in

[94] Article 29 Working Party, 'Guidelines on the right to data portability' WP [2017] 242 rev.01, p. 7 (emphasis ours).
[95] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 *Law, Innovation and Technology* 40, 40-81.; Peter Swire & Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 *Maryland Law Review* 335, 342; Paul M. Schwartz & Daniel J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814, 1873.
[96] See the definition of personal data in Art. 4(1) GDPR: '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'.

practice where market players benefit from applying a uniform approach towards data sharing irrespective of the origin of the regime on which the request is based.

At the same time, the Article 29 Working Party seems to downplay the complexity of situations where individuals can invoke more than one instrument. In its view, the GDPR's data portability provisions only do *not* apply if it is clear from the request that the intention of the individual was to exercise his or her rights under sectorial legislation rather than under the GDPR. An example is given of a data subject specifically aiming at providing an account information service provider access to his or her banking account history. In such cases, access should, according to the Article 29 Working Party, be granted under the provisions of the PSD2.[97] In cases where the request is aimed at portability under the GDPR, it must be assessed on a case by case basis how specific legislation may affect the RtDP. The Article 29 Working Party states that 'the existence of such specific legislation does not override the general application of the data portability principle to any data controller, as provided by the GDPR'.[98] However, no concrete guidance is given on how to determine the relationship between the GDPR and other data sharing regimes. Although the statement of the Article 29 Working Party that specific legislation does not override the GDPR can be understood as implying that the GDPR's RtDP should take precedence, this is not straightforward especially in cases where legislation provides for stronger forms of data sharing in specific sectors. For instance, Article 20 of the Electricity Directive requires final customers to be able to retrieve and port smart meter data 'at no additional cost' whereas the GDPR's RtDP leaves data controllers the option to charge a 'reasonable fee'. Such tensions may lead to disputes about the applicable requirements, in particular as individual consumers will unlikely be aware of the consequences of basing their request either on the GDPR's RtDP or a sector-specific data access tool. At the same time, the GDPR's RtDP can complement the possibilities available under sector-specific data access regimes. For instance, the PSD2 only provides for access-to-account in two instances, namely where third party providers offer either payment initiation or account information services. One may wonder to what extent the GDPR's RtDP can expand the number of situations in which payers can use complementary services building upon their bank accounts. Such a wide interpretation might lead to more data sharing. In addition, as portability implies the physical copying of data to another provider, the GDPR's RtDP can potentially give payers stronger claims versus banks by setting them aside as intermediaries or bottlenecks who control the access to account information.

When operationalising the RtDP, two modalities need to be distinguished: (i) a request by the data subject to receive a copy of the data and transmit it to another controller, and (ii) delegated portability by the data subject to the new controller that is granted the authorisation to extract the data on his or her behalf. It might well be that in the future, the two situations are treated differently for the purposes of compliance. Delegated portability, especially among businesses in the same or similar sectors, might become faster and more standardised through infrastructure. This could mean that even the interpretation of the above opened notions in RtDP will be different depending on *who* is requesting the portability. For instance, what will remain excessive when requested by a data subject, might be considered acceptable when delegated to third parties, although originally concerning the same original controller. The intuition is as follows. The standardisation among businesses might turn delegated portability into a highly automated process, which will reduce the compliance costs of data controllers even in case of repetitive requests. The standardisation might be much more difficult to achieve and

[97] Ibid, p. 7-8 and in particular footnote 15.
[98] Ibid, p. 8.

scale in a relationship with consumers/controllers whose requests might continue to produce higher costs. Such differences in compliance costs could increase the importance of the role of delegated portability for the benefit of business entities, as direct transfers of data to consumers/controllers might remain less 'technically feasible'.

In industries where no additional data sharing regimes are in place, we expect questions about the scope and interpretation of the GDPR's RtDP to mainly relate to whether the right can be invoked to facilitate continuous and repetitive transfers of personal data. This dimension will be key in the effectiveness of the RtDP as a tool to empower data subjects and to facilitate exchange and reuse of data across businesses. It is up to the national data protection authorities and ultimately the Court of Justice to interpret the reach of Article 20 GDPR. The Court of Justice has given expansive interpretations to the scope of EU data protection law before.[99] On the one hand, one may argue that it is not the objective of the GDPR to provide room for follow-on innovation even if this can be a side-effect of some of its provisions, so that sector-specific regulation should be adopted in order to achieve such aims. On the other hand, the policy objective of innovation becomes more difficult to distinguish from the data protection nature of the GDPR, as both also relate to the preservation of the internal market and the free flow of data in the EU.[100]

A data subject will have stronger control over his or her personal data if he or she can freely port it among services at his or her desire. However, without further guidance regarding what is to be considered as 'technically feasible' or 'without undue delay' in terms of complying with a data portability request, data controllers may decide not to adhere to strict standards until an enforcement action of a data protection authority or a judgment of a court imposes such standards on them. This would imply that the requirements of the GDPR's RtDP will differ among industries depending on the presence of additional regimes promoting data sharing. Although differences in implementation across industries are inevitable to a certain extent, the fact that the GDPR constitutes a horizontal data protection regime applicable to all data controllers throughout the economy goes against such sector-specific interpretations. However, as data access and data portability become increasingly accepted and used by individuals as well as businesses, the attitude towards the use and sharing of data may change more generally so that an additional spill-over effect occurs towards other sectors (inter-industry spill-overs) currently not having any additional data sharing requirements in place.

3.4 Price of data use/access

An open term of RtDP that deserves special attention is a 'reasonable fee' which may be charged covering the relevant administrative costs of controllers (Article 12(5) GDPR). Although a number of the sectorial regimes discussed provide for the possibility to charge costs, there are strong indications that one expects the remuneration not to go beyond what is necessary to cover the administrative charges for enabling portability and access. It can be questioned whether this is a good development. The ability

[99] See for instance the *Google Spain* judgment (Case C‑131/12 *Google Spain* [2014] ECLI:EU:C:2014:317) in which the Court of Justice established a right for data subjects to ask for the removal of search results displayed following a search made on the basis of a person's name, before the right to erasure of Article 17 GDPR entered into force.
[100] See Article 1(3) GDPR stating 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'.

of holders of data to ask third parties a fee to access datasets in which they have invested may encourage higher levels of data sharing on the market. In its 2017 Communication on 'Building a European Data Economy', the Commission referred to the possibility of establishing access against fair, reasonable and non-discriminatory (FRAND) terms in analogy to the licensing of standard essential patents.[101] Such fees could be applicable in principle only in business-to-business situations, so that the rights of individuals as data subjects or consumers are not restricted.

Existing data sharing schemes often neglect their interface with potential intellectual property rights of firms involved in the transactions. To the extent that these regimes do not address the issue, and only defer to very general balancing of interests, the use of data might remain to be subject to licensing fees in the future. This is because while the data sharing policies, acting as policy instruments, might force intellectual property holders to relinquish their exclusivity in the process, the right to remuneration may remain the middle ground solution when undertaking the balancing exercise between these policies on the one hand, and the interests of intellectual property holders to benefit from their investments. To avoid any legal uncertainty, it would be advisable that intellectual property rights considerations are resolved much more explicitly within the legal frameworks in order to avoid costly litigation to determine this in the future.[102] Without such reconciliation, the uncertainty will exist about what such framework requires, but also how sectorial laws impact horizontal instruments, like the GDPR's RtDP.

3.5 Policy consequences of spill-overs

This comparative exercise further shows an important dynamic. Policy-makers' decision to pursue horizontal and sectorial data sharing policies in parallel create unintended consequences in their mutual interactions. Some of the spill-overs take place whether the policy-makers consider them or not, while others are only the result of uncertainty and lack of clear direction.

Data portability policies in particular can constitute heavy handed extraction tools which are meant to open up valuable resources held by private parties. They multiply the data across the data ecosystem, thus de facto reduce exclusivity of the resource on the market. Data access policies, on other hand, are more akin to the provision of closely controlled rights to use a unique infrastructure. Unlike extraction tools, which emphasise technical and physical control by their beneficiaries over data for whatever purpose, data access tools focus on the ability to use the building blocks for a particular purpose. They provide its beneficiaries lesser control over the resource but not necessarily control of lower quality. Given their tailoring to a specific use case, they can be faster, smoother and, most importantly, real-time. It is clear that portability and access require a different balancing of interests. However, if one policy has spill-over effects on the other, such balancing might be practically revisited.

Therefore, while data portability and data access are distinct policies, as we tried to show, they are also interrelated. Their data governance influences each other through factual and legal spill-overs. Since data access policies are a result of a much more guided process, they care more about building up the

[101] Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final, p. 13. For an analysis of the notion of FRAND in several EU regimes, see Mathew Heim & Igor Nikolic, 'A FRAND Regime for Dominant Digital Platforms' (2019) 10 *JIPITEC* 38, 45-52.

[102] Considering the situation with intellectual property rights and the RtDP in Article 20 GDRP as illustration of the conflict, see Inge Graef, Martin Husovec & Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal* 1359, 1374 ff.

technical infrastructure necessary for their implementation. Data portability rules that we studied, on the other hand, generally assume existence of such technical infrastructure. If the latter does not exist, portability can be expensive, slow and cumbersome. Data access policies therefore might have important spill-over effects for the GDPR's RtDP. Where their technical infrastructure can be repurposed to allow for portability, extraction might flourish more easily and further stimulate data sharing. Sectorial rules might therefore lead to expansion of the GDPR's RtDP.

This is all the more relevant considering that Member States may decide to adopt more far-reaching data sharing policies. Although this is not a settled issue, the regimes discussed here do seem to leave sufficient scope for Member States to fill in or complement the instruments now available or being developed at the EU level. From the perspective of the internal market as a space where data has to flow seamlessly across borders, such national divergences are not to be welcomed. However, when implementing the data sharing rules set out in EU legislation (especially the Directives which are not directly applicable but have to be transposed in national law), Member States may take advantage of the opportunity to establish links between data portability and data sharing policies in order to provide a more all-encompassing data sharing framework at the national level – especially in terms of the applicable technical infrastructures. The reference to the GDPR's RtDP in Article 20 of the Electricity Directive in the context of portability of smart meter data is instructive in this regard. Eventually, such developments could also be replicated again at the EU level so as to create an overarching approach towards data sharing in the energy sector more generally.

As a result, spill-over effects can travel across different policies and can be bi-directional. Spill-overs can be caused by horizontal policies influencing sectorial, but based on our analysis the intuition is that more often, they will be driven by sectorial policies influencing the horizontal policies. In such cases, the spill-overs can have influence within the original industry of the sectorial law, or even travel further and be expanded to other industries. For instance, one can imagine how requirements for continuous access under a sector-specific regime can influence the interpretation of the GDPR's RtDP through open norms in a way that will eventually also impact how data portability is applied and implemented in other sectors.

4. Conclusion

From the above comparison and analysis, a number of lessons can be derived for the future development of data sharing across sectors. As more industries are becoming digitised and rely on data as input to offer products and services to consumers, the availability of effective portability and access instruments is going become even more important. The successful adoption of innovations within the Internet of Things calls for seamless transfer and exchange of data between businesses, and even between sectors by combining data from different types of services. As a result, it is instructive to explore common or overarching governance trends, particularly with respect to the aspects that can be regarded as key in the configuration of data sharing policies.

Data sharing policies come in different forms (portability or access) for a reason as they try to solve different issues, often for diverging stakeholders. The 'fragmented' legislative strategy pursuing horizontal and sectorial data sharing policies in parallel is therefore fully justified. It should be, however, understood that this strategy also creates unintended consequences in their mutual interactions –

something we termed ‘spill-overs’. These spill-overs might be positive or negative for the welfare of society. Their common feature is that they might expand or contract the original goals/scopes intended by the legislator. Some of the spill-overs take place whether the policy-makers consider them or not, while others are only a consequence of uncertainty and lack of clear direction. For instance, where a sector-specific data access regime leads to the development of a technical standard, this standard can also influence how the GDPR’s RtDP is to be interpreted and implemented in practice. Even though some of these spill-overs can be beneficial in that they create more effective forms of data sharing, legislators should be fully aware of these effects when they pursue a fragmented strategy of data sharing policies. This is particularly the case in the European context because spill-overs might also occur to and from the national level due to local legislation in the Member States.