CLIFFORD

CHANCE

# THE EU DATA ACT PROPOSAL AND ITS INTERACTION WITH COMPETITION, PRIVACY, AND OTHER RECENT REGULATIONS

**An article discussing the EU Data Act proposal and how it intends to regulate IoT-generated data and providers of data processing services, and the competition and privacy issues arising in this context.**

*This article is based on the European Commission's Data Act Proposal dated 23 February 2022.*

# CONTENTS


**Introduction: the EU Data Act and the pursuit of a single market for data** **3**
- The proposal for a "Data Act" fostering data reuse in the EU 3

**Scope of the Data Act proposal** **5**
- The Data Act proposal's keys to data reuse: data access, interoperability and sharing 5
- Data reuse: a complex interplay between competition and privacy 6

**Data access** **11**
- The Data Act proposal: data access 11
- Competition: rights to and enforcement of access to data 12
- How competition and privacy fields have attempted to remedy such concerns by enforcing data access 18

**Data portability and interoperability** **29**
- The Data Act: Data portability and interoperability 29
- Competition: data portability and interoperability 32
- Specific data-related concerns that EU competition law, competition policy, and recent competition law-inspired regulation seek to remedy 32
- How competition and privacy fields have attempted to remedy such concerns by enforcing interoperability and data portability 35

**Data sharing and data pools** **44**
- Data sharing arrangements 44
- The Data Act: data sharing and pooling 45
- Competition law: potential competition concerns which may arise from data pools and data sharing arrangements 46
- Privacy law: potential privacy concerns which may arise from data pools and data sharing arrangements 47
- How competition and privacy laws have attempted to ensure responsible data sharing and pooling and the potential impact of the Data Act in these areas 49
- Data pools and sharing arrangements: impact of the Data Act and Data Governance Act 51

**Future regulatory approach to data** **55**
- Assessing the types of data being used 55
- Data protection impact assessments (DPIAs) 55
- Data stewardship and data trusts 56
- A combined competition and privacy compliance system 56

**Contacts** **59**

# INTRODUCTION: THE EU DATA ACT AND THE PURSUIT OF A SINGLE MARKET FOR DATA

## The proposal for a "Data Act" fostering data reuse in the EU

In 2020, the European Union launched its data strategy, aimed at creating a single market for data (see Legal update, European Commission publishes White Paper on AI and communications on shaping a digital future and European data). The initiative seeks to strike a balance between promoting Europe's global competitiveness and data sovereignty and keeping those who generate data in control of it, by making more data available for use in the EU economy and society. Key elements of the European data strategy include:

- Allowing data to flow freely within the EU.
- Overcoming barriers to data sharing in the EU.
- Fostering the development of collections of sector-specific data.
- Developing a secure, sustainable and interoperable cloud infrastructure for businesses in the EU.

Following the launch of this strategy, businesses investing in data have started reshaping their data governance strategies, enhancing data storage operations in the EU and reconsidering data flows to outside the EU (see, for example, announcements by TikTok and IBM).

A pillar of the EU data strategy is the European Commission's (Commission) proposal for a "Data Act" (the Data Act proposal). Published on 23 February 2022, the proposal sets up rules regarding the use of data generated by Internet of Things (IoT) devices and data collected by cloud services (see Legal update, Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data). The Data Act proposal seeks to ensure equity in the distribution of data value among various stakeholders who deal with data.

The starting assumption of the Data Act proposal is that, while the volume of data generated by humans and machines has increased exponentially in recent years, most data is unused, or its value is concentrated in the hands of relatively few large companies (*see Explanatory Memorandum to the Data Act proposal*, COM(2022) 68 final *(§1)*). This is particularly true in the EU, where, in advance of the publication of the draft, the EU Institutions had been calling for initiatives aimed at unlocking the value of data in Europe by creating a comprehensive regulatory framework that "*facilitates better data portability, fair access to data and ensures interoperability" and "enable[s] better sharing and pooling of data*" (among the key priorities on the EU digital agenda according to the European Council, see EUCO 17/21 and EUCO 13/20, respectively).

In response to these solicitations, and consistent with the objectives of the EU strategy for data, the Data Act proposal establishes a horizontal regulation, aiming to allow data to flow between EU States and across sectors. As such, the goals of the proposed regulation are to:

- Give IoT device users more control over the data they generate and its use.
- Enable use of privately held data by the national and EU public sector bodies in cases of "exceptional" data need.
- Improve switching between cloud and edge services.
- Restrict access by non-EU / non-European Economic Area (EEA) governments to data held in the EU by providers of cloud and edge services.
- Remove barriers to data sharing by developing interoperability standards for data reuse.

# SCOPE OF THE DATA ACT PROPOSAL

The Data Act Proposal covers both personal and non-personal data generated by the use of products and related services (that is, raw machine data), excluding any information acquired through subsequent processing of the raw data (that is, derived or inferred data) (*Article 1(1) and Recital (14)*).

- Under Article 2(2), a product means "*a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*".
- Under Article 2(3), a related service is defined as "*a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*".

Moreover, the broad provision under Article 1(2) covers all sectors, all Business-to-Consumer (B2C), Business-to-Business (B2B) and Business-to-Government (B2G) interactions in the EU and all players active in the data value chain (a concept that describes the evolution of data, from collection to analysis, dissemination, and its final impact on decision making.

## The Data Act proposal's keys to data reuse: data access, interoperability and sharing

The aim of this article is to analyse how the Data Act proposal intends to regulate IoT-generated data. In doing so, it will focus on the legal issues associated with three key aspects:

- Access to data.
- Data interoperability and portability.
- Data sharing and data pooling.

### Access to data

One of the main concerns with regard to data generated by IoT products or related services is that such data is not always easily accessible to users (Recitals (14) and (19), Data Act proposal). This results in users being unable to obtain data necessary to make use of providers of repairs and other services. Access to data by users can therefore be crucial to helping businesses launch innovative, and possibly more efficient and convenient services to address user concerns. Hence, the Data Act proposal establishes legal obligations to make IoT-generated data available, among others, to consumers and businesses (Chapters II to IV). We discuss access to data in Data Access.

### Interoperability and portability

The data access and sharing ambitions behind the EU strategy for data require an interoperability framework capable of enhancing trust and improve efficiency, which the Data Act proposal aims to provide (see Explanatory Memorandum to the Data Act

proposal, COM(2022) 68 final (§1)). Interoperability increases competitiveness and innovation, and ensures sustainable economic growth (Recital (1)). Hence, the Data Act proposal requires compliance with existing open standards and interfaces, and provides for the development of interoperability standards for data to be reused, empowering the Commission to adopt common specifications where necessary to promote interoperability (Chapter VIII). Consistently, it also aims to facilitate the exercise of the right to data portability (Chapter VI), which is already set out under EU law, among others, in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the EU General Data Protection Regulation (GDPR)), broadening such right to include non-personal data. We discuss interoperability and portability in Data Portability and Interoperability.

### Data sharing and data pools

Existing barriers to data sharing prevent an optimal allocation of data to the benefit of society. Data holders lack incentives to enter into data sharing agreements for a number of reasons, among which are uncertainty about the rights and obligations in relation to data, fragmentation of information in "data silos", lack of common data sharing practices and abuse of contractual imbalances with regards to data access and use (Recital (2)). Against this background, the Data Act proposal establishes a framework for data sharing obligations in B2C, B2B and B2G relationships. A key factor that would facilitate data flows within the EU is the creation of large data aggregations and compilations (data pools), consistent with the Council's recommendations (see EUCO 13/20). Depending on the model adopted, data sharing and pooling are potentially useful tools for both monetising data and encouraging data altruism. We discuss the above in Data sharing arrangements.

## Data reuse: a complex interplay between competition and privacy

The effective use and reuse of data can help boost productivity and improve or foster new products, processes, organisational methods and markets, by providing much more information about the preferences and behaviour of individuals (see OECD (2020), Enhancing data access, sharing and re-use, OECD Digital Economy Outlook 2020). Although this enables companies to offer new and better-matching products and services, which increases welfare, it also goes hand in hand with serious concerns that this new information distribution can facilitate data use practices that have the potential to harm individuals and the market as a whole (see Kerber, Wolfgang, Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection (April 26, 2016). Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int) 2016, 639-647).

The preparatory works and the proposed text highlight that the Data Act proposal stems from the EU Institutions' concerns around how data flows within the EU and, ultimately, is monetised. This topic raises a number of competition and privacy issues, including control and transparency of data use, risks of concentrations of data, market entry barriers and abuse of contractual imbalances between the different players in the data value chain.

At the same time, given that a significant portion of the data being processed and monetised by businesses within the EU (and, as far as IoT-generated data falling within the scope of the Data Act proposal is concerned) is personal data, data access, interoperability, portability and sharing under the Data Act proposal provoke further privacy implications.

Therefore, prior to delving into how the Data Act proposal seeks to regulate data access, interoperability, portability and sharing, it is imperative to understand how these topics are relevant to EU competition law, competition policy, and recent competition law-inspired regulation (that is, The Digital Markets Act (Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828) (DMA), and privacy laws (see How are data and related issues relevant to EU competition law, competition policy, and recent competition law-inspired regulation? and How are data and related issues dealt with in privacy law?). While the DMA is not a competition law instrument, it is apparent that its provisions have been inspired by recent EU competition law cases, which the Commission set out in its Impact Assessment Report in relation to each obligation, and aims to complement the enforcement of competition law (Recital 10). It is therefore necessary to consider any potential DMA obligations when considering compliance with competition policy and regulation, and how this interacts with the Data Act proposal and privacy more broadly. It is also crucial to understand what is comprised within the scope of data under these different pieces of legislation (see What is data?).

In light of the above, in the rest of the article, we will therefore discuss competition and privacy issues arising in connection with data access, interoperability, portability and sharing.

### How are data and related issues relevant to EU competition law, competition policy, and recent competition law-inspired regulation?

It is widely acknowledged that data is at the heart of the digital economy (see Furman Report, page 65; Legal update, Digital Competition Expert Panel publishes its report). The ubiquity and non-rivalrous nature of data enables many companies to innovate and compete in ways that hasn't previously been possible. These characteristics open up the field of competition across markets to more players in a potentially unlimited way. Competition policy goals that seek to address data-related concerns recognise that data and digitisation are accelerators for innovation and competition and therefore aim to ensure data is used in the optimal way to realise these benefits. There is widespread acceptance that "digitisation has fundamentally altered the way data is generated, stored, processed, exchanged and distributed… leading to the emergence of new possibilities and business models" (see Commission's final report on Competition Policy for the Digital Era). For example, and as the Commission identified in this report, consumers are able to communicate seamlessly around the world largely for free, accessibility of information has greatly increased, transacting across national borders has been facilitated, consumer choice has increased, and the distribution of cultural goods and news has become much easier. In light of these benefits to consumers and to society "the ability to use data to develop new, innovative services and products is a competitive parameter whose relevance will continue to increase" (see Commission's final report on Competition Policy for the

Digital Era; Legal update, Commission publishes final report on competition policy for the digital era).

While recent focus has been on the role of data within online platforms, search engines, intermediation services and application stores, data is a critical input for production and distribution processes in many industries, such as agriculture, industrial production, logistics, marketing, retailing, and finance (see J. Haucap, Competition and Competition Policy in a Data-Driven Economy, Intereconomics, vol. 54, 2019, no. 4, p. 201-208, citing V. Mayer-Schönberger, K. Cukier: Big Data: A Revolution That Will Transform How We Live, Work, and Think, London 2013, Jon Murray; D.L. Rogers: Digital Transformation Playbook: Rethink Your Business for the Digital Age, 2016, Columbia University Press), and the digitisation of data will revolutionise, in particular, sectors such as mobility and healthcare (see Practical Law: Data use: protecting a critical resource). Given its increasing relevance, numerous reviews and reports both at the EU and national levels have been commissioned to assess data-related competition concerns (see, for example, the Commission's final report on Competition Policy for the Digital Era, the UK's Furman Report, the US House Judiciary Committee's Final Report, and the JFTC's Reports on Algorithms/AI and Competition Policy). These have identified data as a means of raising potential competition concerns, including creating barriers to entry and reinforcing market concentration through network effects; preventing switching and multi-homing, and the resulting consumer lock-in; and providing opportunities for leveraging and self-preferencing. The way in which EU competition law and more recently competition law-inspired regulation such as the DMA have sought to address these data-related issues is set out in Data access: EU competition law and recent competition law-inspired regulation.

### How are data and related issues dealt with in privacy law?

Privacy law focuses on a subset of data, personal data.

Pursuant to Article 4(1) GDPR personal data means "*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*".

The GDPR sets apart and further restricts the processing of the following types of personal data:

Special categories of personal data, that is, "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" (Article 9)*.

Personal data relating to criminal convictions and offences or related security measures (*Article 10*).

Historically, privacy laws have been linked with the data subject's right to be left alone (see *Warren, S. and Brandeis, L. (1890). The right to privacy. Harvard Law Review, Vol. IV, No. 5*).

However, the emergence of the data economy has progressively reshaped the very concept of privacy, from a right to be left alone into a right to *control* data, whereby the data subject has a right to be both aware about who processes their personal data and for what purposes, and in a position to exercise their rights (for example, rectification, erasure, portability, opt-in/opt-out) aimed at preventing the risk of unauthorised data access or use.

The GDPR has in fact acknowledged this new approach to personal data and shifted the dynamics in data processing, by introducing accountability (in lieu of preventive regulatory checks) as one of the pillars of personal data processing and exploitation. As a result of this Copernican revolution in dealing with personal data, we are now at a point where personal data is treated, from many standpoints, like an intellectual property right and is therefore subject to transactions on a daily basis, while privacy rights' enforcement is dealt with before national and supernational privacy authorities and, more recently, civil courts discussing damages arising from breaches of privacy laws.

At the time this article was written, the EU Court of Justice (CJEU) is due to address the issue of whether and under which conditions the GDPR allows data subjects to seek non-material damages following privacy breaches (*UI v Österreichische Post AG (Case C-300/21)*). According to the opinion of AG Campos Sánchez-Bordona delivered on 6 October 2022, infringement alone of the GDPR does not give rise to a right to compensation, unless the data subject suffered actual harm. The outcome of this decision is expected to be a "game changer" in privacy enforcement across the EU, if the CJEU, contrary to the opinion of the Advocate General, opens the door to data protection claims, regardless of whether or not harm occurred.

The Data Act proposal takes another step towards implementing the EU's strategy for a data-driven economy, aiming to narrow the gap between those who carry out data processing ("data controllers" and "data processors") and those whose data is processed ("data subjects") by considering the former as "data holders" and the latter as "users" who can benefit from the processing of the data they generate.

### What is data?

The Data Act proposal applies to "data".

Article 2(1) Data Act proposal defines **data** as "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*". It is undisputed that this definition includes both personal data and non-personal data.

We will hereinafter use the concept of personal data in a restrictive manner, that is, any references to **personal data** will be made in accordance with the GDPR. However, we will use the term **non-personal data** to refer to information that does not fall within the concept of personal data. Finally, references to "data" in a generic sense will include both personal and non-personal data, that is, in line with Article 2(1) of the Data Act proposal.

This distinction is not trivial, as special regulations apply to the processing of personal data. This fact is also acknowledged in Article 1(3) of the Data Act proposal, which states that "*Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation*" and that the Data Act proposal shall not affect the applicable of Union law on the protection of personal data (mainly, the GDPR).

However, the distinction between personal and non-personal data is not always straightforward. It is undisputed that the concept of personal data is very broad (we need only look at the definition under the GDPR) and has also been broadly interpreted (see Article 29 Working Party (WP29), Opinion 4/2007 on the concept of personal data, WP 136). Moreover, it is a changing concept, linked to technology and therefore evolving over time. Thus, in determining what is meant by "identifiable" (one of the most relevant elements of the concept of personal data), the EU legislator has established that all means that may reasonably be used to directly or indirectly identify a natural person must be taken into account. In order to determine "reasonableness", objective factors (for example, identification costs and time) must be addressed, taking into account both the technology available at the time of processing and technological advances (see Recital (26), GDPR). This explains why years ago there was a bitter debate about whether IP addresses (that is, information about an object that can only be linked to a natural person by linking it to other data) did or did not constitute personal data, a debate that is now outdated, even in the case of dynamic IP addresses or IP addresses of computers used in internet cafés (Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14), EU:C:2016:779).

# DATA ACCESS

## The Data Act proposal: data access

Chapters II to V of the Data Act proposal regulate the circumstances under which users, third parties and public sector bodies can access personal and non-personal data:

- Chapter II regulates access to data by users of products or related services (as these terms are defined in the Data Act proposal (see Article 2(2) and 2 (3)) to data generated by them).
- Chapters II to IV regulate access by third parties (B2B) to data generated by products or related services, including access by small and medium-sized enterprises (SMEs).
- Chapter V regulates access to data that is held by the private sector by public sector bodies.

The following sections will set out the competition concerns identified around data access, the means by which the fields of competition and privacy respectively have tried to address such concerns and assess the potential impact of the Data Act proposal provisions in relation to them.

**Chapter II: Business to consumer and business to business data sharing**

- Article 3: Obligation to make data generated by the use of products or related services accessible. Data generated by the use of a product or related service will be directly accessible to the user, who will also be provided with several information regarding the generated data before entering into the contract to use the product.
- Article 4: The right of users to access and use data generated by the use of products or related services. If the data cannot be directly accessible to the user, the data holder will be obliged to make available to the user the generated data by its use of the product or related service.
- Article 5: Right to share data with third parties. In addition, if requested by the user, the data holder will be obliged to share with a third party the data generated by the use of a product or related service.
- Article 6: Obligations of third parties receiving data at the request of the user. In turn, the third party receiving the data shall process the data only for the purposes and under the conditions agreed with the user.

**Chapter III: Obligations for data holders legally obliged to make data available**

- Article 8: Conditions under which data holders make data available to data recipients. In those cases where a data holder is obliged to make data available to a third party (for instance, by virtue of Article 5 of the Data Act proposal), access to the third party shall be granted under fair, reasonable and non-discriminatory terms and in a transparent manner. To that end, the data holder shall follow the provisions of Chapters III and IV of the Data Act (the latter deals with access granted to SMEs).

- The following Articles of Chapter III (Articles 9 to 12) foresee the impossibility of discriminating between comparable categories of data recipients, the prohibition of making the data available to a data recipient on an exclusive basis (unless requested by the user), the terms of the compensation for making the data available, access to dispute settlement bodies as well as the possibility of the data holder to apply protection measures to avoid unauthorised access to the data.

**Chapter IV: Unfair terms related to data access and use between enterprises**

- Article 13: Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise. Paragraph 1 foresees that a contractual term dealing with the access to and use of data or the liability and remedies for the breach or the termination of data related obligations unilaterally imposed by an enterprise to SMEs will not be binding on the latter if it is unfair.
- Paragraphs (2), (3) and (4) provide information of the cases where a clause will be unfair and paragraph (5) establishes the rules to consider that a clause has been unilaterally imposed.

**Chapter V: Making data available to public sector bodies and Union institutions, agencies or bodies based on exceptional need**

- Article 14: Obligation to make data available based on exceptional need. If requested, a data holder will be obliged to make data available to a public body or a Union institution, agency or body if the latter demonstrates an "exceptional need to use the data requested".
- Article 15: Exceptional need to use data. The "exceptional needs" are listed in this Article, and include response to, prevention and assistance to the recovery from public emergencies, and the need of the data so that the public body or Union institution, agency or body can fulfil a specific task in the public interest that has been explicitly provided by law.

## Competition: rights to and enforcement of access to data

Large firms with many users, particularly online platform and intermediation services, data aggregators, social network providers and search engines have come under scrutiny for allegedly collecting vast amounts of data from their users, raising potential concerns around the reinforcement of their market positions, and their ability to use such data to place competing firms (without the same access to data or customers) at a competitive disadvantage. This has led to concerns around market contestability and reduction of potential competition both for and in markets. However, there is also a well-established line of case law, Commission guidance, and an extensive body of academic literature, all of which acknowledge and emphasise the risks around stifling of innovation, reduction of competition in the long-term, and reduction of incentives of a dominant undertaking to invest in areas where competitors are, upon request, able to share the benefits of such investments. EU competition law has therefore set a high threshold for mandating when data must be shared with competitors (see Data access: EU competition law and recent competition law-inspired regulation, below).

### Specific data-related concerns that EU competition law, competition policy, and recent competition law-inspired regulation seek to remedy

Competition law has typically assessed practices relating to the accumulation and use of data under Article 102 of the Treaty on the Functioning of the European Union (TFEU) (see Practice note, Competition regime: Article 102).

### Data is a potential driver of concentration and barriers to entry

Data advantages for incumbents, economics of scale and scope, and network effects have frequently been identified as driving concentration, and creating barrier to entry and expansion, in the digital sector (see Report of the Digital Competition Expert Panel, 2018, page 9). Moreover, according to the DMA Impact Assessment, "there is evidence for a trend of growing market concentration (and, relatedly, growing mark-ups) at the industry level, which has been documented both for the US and for the EU", particularly in the so-called "digital markets". where drivers of concentration can result in a lack of contestability due to high barriers to entry. For instance, a new entrant must convince a sufficient number of users (due to the importance of network effects) to coordinate their migration to a new service, taking, for example, part of the social network along, or other associated data assets such as purchase or preference histories, or ratings (see DMA Impact Assessment, page 9).

"Data-rich incumbents" are cited as being able to reinforce their significant positions by using this data to improve, or make more targeted, their services to users. Strong network effects and externalities created by data, sometimes result in new entrants struggling to acquire a sufficient number of the incumbents' users to migrate to their services. In addition to this, entry can often require access to historical and future user data, which the incumbent may control. This concern is apparent from Commission decisions, the drafting of the DMA (see Digital Markets Act: legislation tracker) and the Commission's final report following its sector inquiry into consumer Internet of Things. For example, in its Google Search (Shopping) decision, the Commission treated Google's data collection advantages as a barrier to entry reinforcing its dominant position (see Legal update, Commission fines Google EUR2.42 billion for abusing dominance by giving illegal advantage to own comparison shopping service):

> "(287) Second, because a general search service uses search data to refine the relevance of its general search results pages, it needs to receive a certain volume of queries in order to compete viably. The greater the number of queries a general search service receives, the quicker it is able to detect a change in user behaviour patterns and update and improve its relevance… The greater the volume of data a general search service possesses for rare tail queries, the more users will perceive it as providing more relevant results for all types of queries."

**The Digital Markets Act** (*Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828*)

The DMA is ex-ante regulation in part informed by European competition law, which came into force on 1 November 2022 and imposes binding obligations on "core platform services" (CPS) operated by "gatekeepers" that are an important gateway for business users to reach end users (and therefore designated as "**Covered Services**") (see Legal update, Digital Markets Act published in the Official Journal). The types of CPS are set out in the DMA, and include, inter alia, online intermediation services, online search engines, online social network services, as well as voice assistants, operating systems, and web browsers (Article 2(2)). Designated "**gatekeepers**" will be firms providing an important gateway CPS for business users to reach end users (that is, a CPS that in the last financial year has at least 45 million monthly active end users established or located in the EU and at least 10,000 yearly active business users established in the EU) where they have significant impact on the internal market (meaning that they achieve an annual turnover in the EU at of least EUR7.5 billion in the last three financial years, or an average market capitalisation of at least EUR75 billion in the last financial year, and provide the same CPS in at least three Member States), and enjoy an entrenched and durable position (*Article 3(1) and (2), DMA*). Even where a firm doesn't meet the quantitative thresholds set out in Article 3(2) of the DMA, it may still be designated a "gatekeeper" by the Commission on account of the factors set out in Article 3(8).

The Commission's impact assessment of the Digital Markets Act pointed to the lack of data access as an important barrier to entry. Recital 36 of the *DMA*, which relates to Article 5(2) on the use of data (see box, DMA), highlights the potential competition concerns which can arise through data accumulation creating barriers to entry. It specifically seeks to address the practices of designated gatekeepers identified below in relation to combining, cross-using and signing-in users to further consolidate the wealth of data they possess. Recital (36) explains that:

> "[g]atekeepers often directly collect personal data of end users for the purpose of providing online advertising services when end users use third party websites and software applications. Third parties also provide gatekeepers with personal data of their end users in order to make use of certain services provided by the gatekeepers in the context of their core platform services, such as custom audiences. The processing, for the purpose of providing online advertising services, of personal data from third parties using core platform services gives gatekeepers potential advantages in terms of accumulation of data, thereby raising barriers to entry. This is because gatekeepers process personal data from a significantly larger number of third parties than other undertakings. Similar advantages result from the conduct of (i) combining end user personal data collected from a core platform service with data collected from other services, (ii) cross-using personal data from a core platform service in other services provided separately by the gatekeeper, notably services which are not provided together with, or in support of, the relevant core platform service, and vice-versa, or (iii) signing-in end users to different services of gatekeepers in order to combine personal data."

These potential competitive concerns have been reiterated by the Commission in relation to the IoT sector. On 16 July 2020, the Commission launched a sector inquiry into the consumer IoT (see Legal update, Commission opens consumer Internet of Things sector inquiry). In its final report published in January 2022, the Commission noted that privileged access to huge data volumes might enable leading voice assistant operators to more easily improve through machine learning. Not having access to this data can raise barriers for new entrants (see Legal update, European Commission publishes final report in consumer Internet of Things sector inquiry).

### Leveraging and self-preferencing

Potential competition concerns under Article 102 of the TFEU may also arise in relation to a dominant undertaking's alleged ability to accumulate third-party generated data, as it is argued that this can give it a competitive advantage. Such leveraging could be either "offensive" (that is, to generate more profits) or "defensive" (that is, preventing entry in the core market from an adjacent, often niche, market) (see Competition Policy for the Digital Era Final Report, page 7). This typically arises where an undertaking is vertically integrated across two markets, and therefore has a purported "dual-role". The Commission has launched two recent investigations into practices which it believes raises such concerns.

- **Cross-use of data acquired across different services.** Vertically integrated companies have been accused of using data acquired from their customers by virtue of their position on one market, to purportedly "leverage" this in competition with third parties on an adjacent market. For example, on 17 July 2019, the Commission opened a formal investigation to assess whether Amazon's use of non-public data from independent retailers selling in its marketplace breached EU competition rules (Case AT.40462 Amazon Marketplace (see Legal update, Commission sends statement of objections to Amazon about use of seller data and opens second investigation into Amazon's e-commerce business practices)). On 10 November 2020, the Commission issued a statement of objections outlining its preliminary view that Amazon abused its dominant position by using non-public seller data to focus its own offers on the best-selling products, avoiding normal risks of retail competition and leveraging its dominance in the marketplace (see Commission Press Release 10 November 2020).
- **Google, AdTech and Data-related practices.** On 22 June 2021, the Commission has also opened an investigation into Google's practices which allegedly favour its own online display advertising technology services (Case AT.40670). Specifically, Google has been accused of restricting third parties' access to user data for advertising purposes on websites and apps, while reserving such data for its own use (see Press Release and Case tracker, Google: Adtech and Data-related practices). Margrethe Vestager has voiced concerns, stating that "*Google collects data to be used for targeted advertising purposes, it sells advertising space and also acts as an online advertising intermediary. So Google is present at almost all levels of the supply chain for online display advertising. We are concerned that Google has made it harder for rival online advertising services to compete in the so-called ad tech stack*." Notably, in its Press Release, the Commission indicated that it will take into account the need to protect user privacy, in accordance with EU laws such as the GDPR, highlighting that "[c]*ompetition law and data protection laws must work*

*hand in hand to ensure that display advertising markets operate on a level playing field in which all market participants protect user privacy in the same manner*".

Such concerns are also reflected in Recital (46) of the DMA, which identifies and highlights the specific issues which arise when an undertaking has a dual-role whereby it provides a "*core platform service*" on which business users are active, and also competes with such business users on this adjacent market. It states that "*In those circumstances, a gatekeeper can take advantage of its dual role to use data, generated or provided by its business users in the context of activities by those business users when using the core platform services or the services provided together with, or in support of, those core platform services, for the purpose of its own services or products*."

**Internet of Things.** In its final report on the IoT sector enquiry, the Commission noted concerns that voice assistants are central to data collection and that providers of these devices can control both data flows and user relationships. The Commission also found that leading voice assistant providers could leverage those advantages in other markets to the detriment of third-party manufacturers and service providers (see Legal update, European Commission publishes final report in consumer Internet of Things sector inquiry).

Storing and collecting personal data through the application of terms and conditions which allow cross-use and combining of data across different sources: Competition investigations and regulator sector studies have reported the imposition of terms and conditions on users making the use of an undertaking's services conditional on being able to collect and combine their data from multiple sources (see *EU Impact Assessment support study, Stigler Center report, page 44, US - House Judiciary Committee report "Investigation of Competition in the Digital Marketplace: Committee Report and Recommendations*").

For example, the UK's Competition and Markets Authority (CMA) has expressed concerns that online platforms require users to agree to significant use of their data across different parts of the business as part of their initial use, often through use of "clickwrap" agreements which inappropriately aggregate consent. For example, Google and Microsoft aggregate consents across all their services where a consumer chooses to sign up to any one of their individual services and combine data across their services and products, as confirmed in their privacy policies (see CMA report on Online platforms and digital advertising, pages 188-193). National competition authorities (NCAs) have found such practices to constitute an abuse of a dominant position under national competition law (see Exploitative abuses through use of data: Restrictions on collection of personal data, below) (German NCA decision B6-22/16) finding Facebook applied terms and conditions making use of its network conditional on being able to collect and combine user data from multiple sources and Italian NCA decisions on 11 May 2017 against WhatsApp forcing users to share personal data with Facebook). Undertakings have also been found to require users to sign up to or register for its services (for example, app stores, operating systems, social networks) using its own email services, allegedly enabling them to combine data from several sources (see DMA Impact Assessment, *page 11*).

**Automatic sign-in / authentication to collect data across services.** Related to this, in certain "digital ecosystems", it has been found that signing into one service provided by a firm, will automatically sign users into its other services, enabling the collection and combining of data across services. For example, the US House Judiciary Committee's Final Report on Competition in the Digital Marketplace highlighted Google's integration of its Chrome browner with other Google products, such that signing into Chrome automatically signed users into Gmail, YouTube, and additional Google services, helping Google "*build more detailed user profiles by connecting activity data to the user's Google Account*".

### Restricting competitors' access to data

This practice can take two forms:

- Restricting competitors' access to data that a dual platform has accumulated by virtue of its strong market position (for example, Google Search (*Shopping*) and refusal to deal case law below).
- Preventing a dual platform's business users (who are also often competitors) from accessing data generated by such business users' through transactions with end users on the dual platform. For example, online platforms have been reported to impose authentication through the platform even when third party services/products are used, to create a direct link with customers to the detriment of third-party providers by restricting their access to this data (that is, "disintermediation") and preserving "monopoly access to user data" (*see* Commission's impact assessment of the Digital Markets Act, *page 30*).

Consumer welfare considerations of self-preferencing: Self-preferencing is still a relatively novel theory of harm and by no means necessarily detrimental to consumer welfare. Notably, the Commission has settled *Amazon Marketplace* by way of commitments without finding that the alleged use of data amounted to anti-competitive conduct (for example, anti-competitive self-preferencing, or leveraging more generally). Additionally, the Commission is yet to issue its decision (if any) in Google, AdTech and Data-related practices.

Recent economic theory has found that "there are strong indications that some platforms engage in practices that may be called self-preferencing, but that this is not always consumer welfare detrimental" (see CERRE: The Prohibition of Self-Preferencing in the DMA). This paper suggests in fact that prohibiting self-preferencing may in some circumstances be detrimental to consumer welfare. CERRE have identified that where firms operate in "dual mode" (that is, selling first-party products on its platform where third party products are sold), a self-preferencing prohibition increases consumer welfare under some conditions. Particularly in markets with little competition between third-party sellers, firms may be understandably concerned about their consumers receiving a bad deal and therefore would be inclined to introduce a first-party product (in particular where it has a cost or quality advantage over third-party sellers) to stimulate competition. For example, another economic study has found that Amazon's first-party retail entry "is associated with modest positive effects on both consumer and third-party merchant outcomes more consistent with mild market expansion than with appropriating third-party sales" (see *Crawford, G., M. Courthood, R. Seibel, and S. Zuzek (2022)*, Amazon entry on Amazon Marketplace, *CEPR*

*Discussion Paper DP17531*). CERRE find the "dual mode" always produces higher consumer welfare than a "pure marketplace", and that a ban on the "dual mode" never increases consumer welfare. This is important to consider when assessing how competition law and policy approaches self-preferencing, as burdensome self-preferencing remedies and the legal risks associated with increased regulation may lead firms to opt out of and avoid the dual mode altogether (see CERRE: The Prohibition of Self-Preferencing in the DMA).

## How competition and privacy fields have attempted to remedy such concerns by enforcing data access

### Data access: EU competition law and recent competition law-inspired regulation

#### Granting access to data: duty to supply and the essential facilities doctrine

Traditionally, EU competition law has sought to remedy concerns around barriers to entry and leveraging that can arise from the accumulation of and access to data, under the Article 102 TFEU framework. In particular, the Commission has done so using the "essential facilities" doctrine and refusal to deal line of case-law (see Practice note, Competition regime: Article 102: refusal to supply and essential facilities). EU competition law sets a very high threshold for when dominant firms must share their property with competitors. For "classical" infrastructure, the Bronner criteria must collectively be satisfied for a refusal to supply to constitute an abuse:

- The refusal must likely to eliminate all competition on downstream market.
- Access must be indispensable to carrying on the other undertaking's business, meaning that there is no actual or potential substitute available.
- A refusal must be incapable of objective justification.

As commented in that case, "*[i]n the long term it is generally pro-competitive and in the interest of consumers to allow a company to retain for its own use facilities which it has developed for the purpose of its business. For example, if access to a production, purchasing or distribution facility were allowed too easily there would be no incentive for a competitor to develop competing facilities. Thus while competition was increased in the short term it would be reduced in the long term. Moreover, the incentive for a dominant undertaking to invest in efficient facilities would be reduced if its competitors were, upon request, able to share the benefits. Thus the mere fact that by retaining a facility for its own use a dominant undertaking retains an advantage over a competitor cannot justify requiring access to it.*" (Opinion of AG Jacobs delivered on 28 May 1998 in CJEU case C-7/97, Bronner, paragraph 57).

Subsequent case law has extended to licensing intellectual property rights (IPRs) to competitors, however only in "exceptional circumstances" (CJEU judgement of 6 April 1995, joined cases C-241/91 and P and C-242/91 P, RTE and ITP v Commission (Magill)). For a refusal to license IPRs to constitute an abuse, in addition to the Bronner criteria, the data or input held by the dominant firm must be essential to the appearance of a "new product" (see Practice note, Transactions and practices: EU Intellectual property transactions: Refusal to grant a licence to any third party at all).

That being said, some commentators argue that the European Court somewhat relaxed this stringent requirement in Microsoft, by requiring only that the input be essential for "follow-up innovation" (which in turn may result in the appearance of a new product in the future) (see Practice note, Competition regime: Article 102: refusal to supply and essential facilities).

In its guidance on Article 102 of the TFEU, the Commission explicitly acknowledges the high threshold and careful consideration competition law requires for mandating access and sharing of property:

> "[w]hen setting its enforcement priorities, the Commission starts from the position that, generally speaking, any undertaking, whether dominant or not, should have the right to choose its trading partners and to dispose freely of its property. The Commission therefore considers that intervention on competition law grounds requires careful consideration where the application of Article [102] would lead to the imposition of an obligation to supply on the dominant undertaking. The existence of such an obligation - even for a fair remuneration - may undermine undertakings' incentives to invest and innovate and, thereby, possibly harm consumers. The knowledge that they may have a duty to supply against their will may lead dominant undertakings or undertakings who anticipate that they may become dominant - not to invest, or to invest less, in the activity in question. Also, competitors may be tempted to free ride on investments made by the dominant undertaking instead of investing themselves. Neither of these consequences would, in the long run, be in the interest of consumers" (paragraph 75).

Commentators have questioned the applicability of Article 102 of the TFEU when access to data is required or requested. As data can often be replicated and acquired from a range of sources (that is, it is non-rivalrous), it is uncertain whether access to data can be considered "indispensable", as is required to satisfy the Bronner criteria (see Article, Data use: protecting a critical resource). The Commission has also recognised this and observed that whether and, if so, when the refusal of a dominant firm to grant access to data may result in an abuse of dominance, is a "heated debate". Therefore, particularly in the context of "digital markets", existing competition law (that is, Article 102 of the TFEU) may not be adequate to remedy the potential data-related concerns noted above (see *the Commission's final report on* Competition Policy for the Digital Era).

Outside of online platforms and "Big Tech", ongoing investigations across sectors are also challenging the question of when dominant firms must share data with their rivals. For example, in the railway / transport sector, the German NCA has charged Deutsche Bahn (Europe's largest railway operator) with abuse of dominance, by giving data to its own mobility platform (where consumers can purchase tickets) while refusing to share it with some rivals. The German NCA is pursuing the case under both EU law (and therefore the refusal to deal case law), which sets a higher threshold than the equivalent national standard, and German national competition law, and commentators are waiting to see whether this may set a new precedent for dominant undertakings' data sharing obligations.

**DMA**

The perceived shortcomings of existing competition law to remedy data related concerns have led to the DMA imposing new obligations on "gatekeepers" requiring them to give competitors and end users access to different types of data. Gatekeepers whose search engines are listed in their designation decision will need to provide rivals with fair, reasonable and non-discriminatory (FRAND) access to user-generated search query, click and view data (although any personal data will need to be anonymised) (*Article 6(11)*). Gatekeepers will also have to provide business users and third parties authorised by them with access to data that is generated by those business users (and their customers) on the CPS, or another service offered with, or supporting, the CPS (*Article 6(10)*).

Many commentators welcome these provisions as providing the necessary tools to maintain market contestability. However, other commentators and technology companies have questioned whether the obligations imposed by the DMA are appropriate, especially taking into account the reasoning behind the high threshold and careful analysis competition law (*as set out in Bronner and Magill*, for example) requires for before imposing information and data-sharing obligations. Ohlhausen and Taladay have emphasised that the "drive to modify competition laws to address digital markets does not justify an abandonment of core competition principles" (see Maureen K Ohlhausen, John M Taladay: Are Competition Officials Abandoning Competition Principles). Insofar as investment and scale are necessary to facilitate innovations which improve these data-driven services, it is yet to be seen whether such free and unencumbered access rights for competitors will reduce incentives for research and development, and the corresponding investments, to the detriment of end-consumers. For example, the Information Technology and Innovation Foundation (ITIF), the European Policy Information Centre (EPIC), and the Centre for European Reform (CER) have raised such concerns and question the implications of the DMA for innovation and flexibility (see Aurélien Portuese, ITID: The Digital Markets Act: European Precautionary Antitrust; EPIC: The Digital Markets Act: Precaution over Innovation; and Zach Meyers, CER: No pain, no gain? The Digital Markets Act). Competition law is able to assess on a case-by-case basis when companies using data generated through their services to promote or improve their other services is in fact anti-competitive after balancing these competing considerations. However, these commentators note that ex ante regulation like the DMA is arguably neither flexible nor nuanced enough to reflect and promote these consumer-welfare enhancing factors sufficiently, and represents the triumph of the "precautionary principle" that runs counter to and is detrimental to introducing new products, processes, and business models - in short, in disrupting an economy in need of disruption, particularly in Europe (see Aurelian Porteuse, Information Technology and Innovation Foundation: The Digital Markets Act: European Precautionary Antitrust).

### Concerns of self-preferencing and leveraging through use of data: restrictions on use of and collection of data by undertakings

Under Article 102 of the TFEU, leveraging abuses are found where a dominant undertaking exploits its position of market power on one market by engaging in abusive practices which have actual or potential anti-competitive effects on a different market. As such, competition law has been utilised to remedy the possible concerns which may arise from firms being able to collect and use data in the ways set out above that may have the effect of leveraging and extending dominance across markets.

Outside of the digital realm, competition law has been used to address "data-leveraging" practices in relation to datasets. In Servizio Elettrico Nazionale, the Italian NCA found that the Enel Group used data obtained by virtue of its post-monopoly dominant position to engage in an exclusionary strategy "designed to transfer" SEN's customer base (SEN being the operator on the protected market) to EE (active on the free market) (see Legal update, Advocate General opinion on criteria for classifying an exclusionary practice as an abuse of a dominant position (ECJ)).

As explained above, the Commission has alleged that Amazon's dual-role gives it access to data about independent sellers' activities on its online marketplace, including non-public business data. It has relied on Article 102 of the TFEU in taking the preliminary view that "*the use of non-public marketplace seller data allows Amazon to avoid the normal risks of retail competition and to leverage its dominance in the market for the provision of marketplace services in France and Germany*" (see European Commission Press Release, Antitrust: Amazon). It is notable, however, that Amazon has offered and the Commission has accepted commitments to remedy any potential concerns, and therefore such data-related practices have not yet been found to amount to an abuse of dominance under Article 102 or breach of competition law. Amazon has committed to refrain from using non-public data relating to, or derived from, the activities of independent sellers on its marketplace, for its retail business that competes with those sellers (see Legal update, Commission seeks feedback on commitments offered by Amazon to address competition concerns about marketplace seller data and access to Buy Box and Prime). Commentators have observed that elements of these commitments mirror the obligations set out in Article 6(2) of the DMA, and therefore this may have important implications for both the interpretation of the DMA and how competition law is brought in line with this regulation.

**DMA**

In light of the difficulties traditional competition law has in effectively remedying such data-related practices, Article 6(2) of the DMA explicitly seeks to prevent these practices, that is, gatekeepers who compete with their business users must not use data generated by these businesses and their users on the CPS, or another service offered with or supporting the CPS.

Equally, Article 5(2) prohibits designated gatekeepers from combining or cross-using personal data from a CPS with person data from any other service of the gatekeeper without specific user consent in an effort to prevent potential leveraging by virtue of have dual-access to such data

### Exploitative abuses through use of data: restrictions on collection of personal data

Restrictions on collection of data: While restrictions on how firms can collect and use, in particular, personal data has traditionally been considered under the lens of data protection and privacy law, in February 2019, the German NCA found Facebook's application of terms and conditions making use of its network conditional on being able to collect and combine user data from multiple sources constituted an exploitative abuse of its dominant position under national competition law (German NCA decision delivered on 6 February 2019, B6–22/16). This was the first time a competition authority had explicitly taken into account the protection of privacy and privacy law requirements when applying competition law (see Kerber, W., Zolna, K.K. The German Facebook case: the law and economics of the relationship between competition and data protection law. Eur J Law Econ 54, 217–250 (2022)). Specifically, the Federal Cartel Office (FCO) found that "being a manifestation of market power", the terms and conditions Facebook applied violated the GDPR and were therefore abusive within the meaning of the applicable provision under German competition law.

This approach seems to be reflected in the DMA, which considerably restricts how designated gatekeepers can use the data gathered through their various activities due to the competition concerns identified above (see, in particular, Recital (36)). Under Article 5(2) of the DMA, without specific user consent, designated gatekeepers must not combine or cross-use personal data from a CPS with personal data from any other service of the gatekeeper. Gatekeepers should also obtain consent to use, for advertising purposes, the data collected from end users through their usage of, for example, third-party apps and websites. Repeated cookie banners requiring consent will also likely be banned, as the gatekeepers cannot request consent more than once in a year if consent has already been refused (see Clifford Chance briefing, The Digital Markets Act: A new era for the digital sector in the EU). This obligation appears to reflect the concerns of the FCO and mirrors its proposed remedy, indicating the potential influence of the GDPR within competition law enforcement going forward. From a data protection and privacy law perspective, Article 5(2) of the DMA, which is lex specialis vis-à-vis the GDPR, contains a list of processing activities related to online advertising and combination of personal data from different sources for which consent will be required. Therefore, gatekeepers will not be allowed to process personal data for these purposes on the basis of an alleged legitimate interest, or another legal basis for the processing under Article 6(1) GDPR, and will be obliged to rely on consent.

### Data access: privacy perspective

The Data Act proposal foresees that its provisions are coherent with the existing rules on the protection of personal data (mainly, the GDPR). Therefore, as far as the term "data" under the Data Act proposal comprises personal data, EU law on the protection of personal data will continue to apply to any access, use and sharing of such personal data, since all three fall within the scope of "processing" of personal data pursuant to Article 4(2) of the GDPR (as confirmed by *Article 1(3), Data Act proposal and Explanatory memorandum (§ 1)*). While in some cases the Data Act proposal will overlap with applicable privacy law, its application cannot imply putting the data subject in a worse position than the one vested by privacy law. In light of this, the Data Act proposal includes several paragraphs which are completely in line with the principles and obligations of the GDPR.

### Access to data by users of connected devices to data generated by them

The Data Act proposal has provided for scenarios where there could be potential conflict between access by users to data (personal data) generated by the use of products or related services under Articles 3 and 4 Data Act proposal and access under the GDPR provisions.

In cases where the user is the data subject, that is, where the user of the product or related service is requesting access to his/her own data (including personal data), the GDPR already foresees an access right which entitles the data subject to contact the data controller to ascertain whether or not it is processing its personal data and, if so, to obtain certain information about the processing as well as a copy of (that is, access to) the personal data processed (*Article 15, GDPR*).

Under Article 2(5) of the Data Act proposal, user means "*a natural or legal person that owns, rents or leases a product or receives a services*".

A data subject under the GDPR refers to a natural person to whom the personal data relates and who can be identified, directly or indirectly, by reference to that personal data (*Article 4(1), GDPR*) (see Practice note, Overview of EU General Data Protection Regulation).

The access right under the GDPR covers not only the personal data provided by the data subject to the data controller, but also the personal data generated by the data controller by the data subject's use of a product or related service (see EDPB Guidelines 01/2022 on data subject rights - Right of access, page 31).

Even though the scope of the access right under the Data Act proposal is broader than the access right under the GDPR (for instance, the Data Act proposal sets out an obligation under Article 3(2) to provide certain information, such as the nature and volume of the data likely to be generated by the use of the product or related service, to the user before concluding a contract for the purchase, rent or lease of the product or related service), these additional rights would not undermine the data subject's privacy, as access to his/her own data cannot negatively affect their right to privacy.

Additionally, there can be cases where the user (that is, the individual who requests access under the Data Act proposal) is not the data subject. In those cases, the right to privacy of the data subject could be at risk, as another individual (that is, the user) could gain access to their personal data. The Data Act proposal already foresees this scenario in Article 4(5), which states that in these cases the personal data generated by the use of the product or related service will only be made available to a user who is not the data subject if a legal basis for the processing exists (for instance, the data subject's consent) and, where the personal data includes special categories of personal data, the stricter conditions under Article 9(2) of the GDPR are met.

The legal bases for personal data processing are those scenarios that justify a processing of personal data. The legal bases are listed in Article 6 of the GDPR: consent; performance of a contract; compliance with a legal obligation; vital interests; public interest and legitimate interest.

As regards special categories of personal data, pursuant to Article 9(2) of the GDPR, a data controller may process such data if, in addition to a legal basis for the processing, one of the following conditions applies: explicit consent; employment, social security and social protection (if authorised by law); vital interests; not-for-profit bodies; made public by the data subject; legal claims or judicial acts; reasons of substantial public interest (with a basis in law); health or social care (with a basis in law); public health (with a basis in law); and archiving, research and statistics (with a basis in law).

Any processing of personal data (in the above example, the transfer of personal data to the user) is subject to the principle of lawfulness provided by Article 5(1)(a) of the GDPR and must be covered by one of the six legal bases under Article 6 of the GDPR. Although it is the responsibility of the data controller to choose which of the six legal bases for the processing fits better, the ones most likely to apply in the above scenario would be the data subject's consent or the existence of a legitimate interest pursued by the data controller or a third party (for example, the user).

Furthermore, Article 4(2) of the Data Act proposal includes other provisions that show that the European legislator has taken the GDPR's principles into account when drafting the proposal:

- Prohibiting the data holder from requiring the user to provide any information beyond what is necessary to verify their quality as user. This is in line with the data minimisation principle, which states that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (*Article 5(1)(c), GDPR*). This situation has been addressed by the European Data Protection Board (EDPB) in other scenarios that are comparable to the one at hand, for instance, in the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, where it is acknowledged that "age verification should not lead to excessive data processing".
- Prohibiting the data holder from keeping "any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure", consistent with the storage limitation principle: personal data shall be kept for no longer than necessary for the purposes for which the personal data are processed (*Article 5(1)(e), GDPR*).

### Access to data by third parties (B2B)

Access to data (personal data) by third parties at the user's request (Article 5 Data Act proposal) is also consistent with the GDPR.

The premise in this case is that granting access to personal data to a third party amounts to processing of personal data which needs to be covered by one of the legal bases of Article 6 of the GDPR. That said, two situations can be distinguished:

- First, when the user who requests access by a third party is the data subject of the personal data that will be made available to the third party. In these cases, consent of the data subject could be the applicable legal basis. Having said that, the data holder (transferor) will have to bear in mind the accountability principle under Article 5(2) of the GDPR and keep proof of the data subject's request, the information provided to the data subject regarding the conditions under which access will be granted to the third party and ensure that the transfer is made applying appropriate technical and organisational measures (*Article 5(1)(f), GDPR*).
- Second, when the user who requests access by a third party is not the data subject of the personal data that will be made available to the third party. This potentially puts the right to privacy of the data subject at risk. However, Article 5(6) of the Data Act proposal has taken care of this situation and has established that the personal data will only be transferred to the third party if a legal basis for the processing exists and, where the personal data includes special categories of personal data, the conditions of Article 9(2) of the GDPR are met.

Again, the most likely legal bases to be applicable to the processing (that is, to the transfer of the personal data) would be the data subject's consent or the existence of a legitimate interest pursued by the data controller or a third party (for example, the user who requests access by the third party or the third party).

A third party granted access to personal data, is required to comply with Article 14 of the GDPR, which establishes the obligation of the data controller (the third party receiving the personal data) to provide the data subject with certain information on the processing of their data, where the personal data has not been obtained from the data subject itself. The information to be provided under Article 14 of the GDPR includes, among others, the existence of profiling activities that affect the data subject.

However, taking into account that, as anticipated, EU law on the protection of personal data will continue to apply, the third party could also undertake profiling activities if it has obtained the data subject's consent (Article 6(1)(a), GDPR). Needless to say, the consent would need to be valid, that is, it must be a manifestation of free, specific, informed and unequivocal will (Article 7, GDPR).

Under Article 4(4) of the GDPR, profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

According to Article 6(2)(b) of the Data Act proposal, the third party shall not use the data received "*for the profiling […] unless it is necessary to provide the service requested by the user*".

### Access by public sector bodies to data that is held by the private sector and that is necessary for exceptional circumstances

This transfer of data (personal data) to public sector bodies or Union institutions, agencies or bodies also constitutes processing of personal data and therefore needs to be covered by a legal basis under the GDPR.

Given that access to personal data will be granted to public sector bodies on the basis of an "exceptional need", the most likely legal bases under the GDPR that would justify access would be the following:

- Processing is necessary for the performance of a task carried out in the public interest (*Article 6(1)(e), GDPR*), which covers situations where the controller itself has an official authority or a public interest task (but not necessarily also a legal obligation to process data) and the processing is necessary for exercising that authority or performing that task. This legal basis potentially has a very broad scope of application and, therefore, is the most likely scenario (see WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, adopted on 9 April 2014).
- We cannot discard the application of Article 6(1)(d) of the GDPR, that is, the processing is necessary to protect the vital interests of the data subject or of another natural person, mainly in those cases where the personal data is requested to respond to, prevent or assist the recovery from a public emergency. Although this legal basis is of limited application, it could be applied to public emergencies of life and death or, at least, "threats that pose a risk of *injury or other damage to the health of the data subject*" (see *WP29, Opinion 06/2014*).

Lastly, there are other provisions of the Data Act proposal which are perfectly aligned with the principles of the GDPR. For instance, Article 19(1) establishes that the public sector body or EU institution, agency or body receiving the personal data shall:

- "Not use the data in a manner incompatible with the purpose for which they were requested".
- "Implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects".
- "Destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data have been destroyed".

These provisions are no more than a reflection of the purpose limitation, integrity and confidentiality and storage limitation principles provided under the GDPR.

### Data access: impact of the Data Act proposal on competition and privacy fields

#### Competition

Mandating data sharing and access under the Data Act proposal is limited to users and manufacturers (the latter being data holders) of connected devices, and specified circumstances. It is not intended to rewrite competition policy wholesale but strike a balance with promoting competition in these aftermarkets, where currently only the primary service or product provider can operate as small-to-medium-sized business

struggle to obtain access to data. In this way, the Data Act proposal may address the potential competition concerns the Commission has identified in relation to IoT (that is, manufacturers and providers of IoT devices may have privileged access to the data accumulated via these devices, not only creating potential barriers to new entrants but raising the possibility for incumbents to engage in anti-competitive leveraging and self-preferencing), by giving users the ability to ensure their data cannot be used in this way. Its application more broadly, however, is restricted by design. While certainly aiming to promote competition, notably, Article 88 makes it clear that the Data Act proposal should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the TFEU.

The DMA seeks to resolve the issue of dual platforms having an unfair, competitive advantage in competing with their customers, as it obliges designated gatekeepers to share data with third parties that are business users of their CPS; whereas the Data Act proposal goes one step further in promoting competition for start-ups and SMEs in the aftermarket by imposing an obligation to provide data (upon a user's request) to *any* third party (with the exclusion of firms designated as "gatekeepers" under the DMA being beneficiaries of Chapter II). In this specific context, the Data Act proposal's obligations appear broader than both existing competition law and the DMA.

Recital (36) Data Act proposal explains: "*Start-ups, small and medium-sized enterprises and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach. At the same time, a small number of very large companies have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them... The [*DMA*] aims to redress these inefficiencies and imbalances by allowing the Commission to designate a provider as a "gatekeeper", and imposes a number of obligations on such designated gatekeepers, including a prohibition to combine certain data without consent, and an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679 [i.e. the GDPR]. Consistent with the [DMA] and given the unrivalled ability of these companies to acquire data, it would not be necessary to achieve the objective of this Regulation, and would thus be disproportionate in relation to data holders made subject to such obligations, to include such gatekeeper undertakings as beneficiaries of the data access right. This means that an undertaking providing core platform services that has been designated as a gatekeeper cannot request or be granted access to users' data generated by the use of a product or related service or by a virtual assistant based on the provisions of Chapter II of this Regulation*".

Under the Data Act proposal, the B2B sharing of data must be **at the request of the user**. In light of this, it does not envisage mandating private data-sharing in a way which would conflict with or override the existing competition law position on when a dominant firm must grant a competitor access to data it has accumulated (outside of the IoT realm). It is noted that the provisions of the Data Act proposal require data

holders to make data available to public sector bodies in cases of exceptional need, however this is not a mechanism to reform or overhaul the competitive dynamics of a sector by making data available to competitors. Moreover, the Data Act proposal directly prohibits users from using this data to develop competing connected and related devices. Competition law, particularly in relation to refusals to grant access to data (and other property), is utilised in cases where firms wish to use this as an input to develop competing products or services, and steps in to ensure market contestability to the benefit of consumers. Given the Data Act proposal's stated prohibition, it is limited in facilitating the type of access to data which companies make use of competition law to provide. The DMA already represents a significant shift from the existing restrained approach to mandating data sharing under traditional competition law, and outside of the IoT realm, this will have a far greater impact. Furthermore, the Data Act proposal does not regulate potential self-preferencing data-related practices or mandate how data is collected in the ways which have been identified as giving rise to potential competition concerns above.

### Privacy

Although the provisions dealing with access to data foreseen in the Data Act proposal have an obvious impact on privacy (as mentioned, data may comprise personal data and access means processing of personal data in the majority of cases) the provisions of the Data Act proposal seem to be coherent with the GDPR. Having said that, transferors of (personal) data, that is, those who grant access, and transferees (those to whom access is granted), either private or public bodies, will have to actively analyse whether the access to data comprises access to personal data and, if so, assess which obligations and principles need to be complied with in order to make the access completely compatible with the GDPR. This may imply considering legal bases for the processing, information obligations, implementation of technical and organisational security measures to ensure an appropriate level of security and compliance with all the principles set forth in the GDPR.

# DATA PORTABILITY AND INTEROPERABILITY

## The Data Act: Data portability and interoperability

As explained above, the Data Act proposal recognises that the right to use data is valuable. According to the Commission, the true potential of this value is not being realised for reasons including "*lack of clarity regarding who can use and access data generated by connected products, the fact that SMEs are frequently not in a position to negotiate balanced data-sharing agreements with stronger market players, barriers to switching between competitive and trustworthy cloud and edge services in the EU, and the limited ability to combine data emanating from different sectors*". In its Impact Assessment Report for the Data Act proposal, the Commission explained that the overall problem the Data Act proposal tackles is the insufficient availability of data for use and reuse in the European economy or for societal purposes. The proposal therefore aims to achieve fairness in the allocation of value among the players in the data economy, by fostering access to and use of data in a context characterised by the proliferation of cloud services and IoT.

The Commission found that there is legal uncertainty among consumers and businesses concerning data access and use, and this uncertainty also pertains to data portability and interoperability (see Data Act proposal Impact Assessment Report, page 15). The scope of the existing portability right under Article 20 of the GDPR and the technical means of ensuring interoperability are unclear. Data portability and interoperability have therefore been identified as key drivers to achieving the Data Act proposal's goal of data use and reuse, and the proposal includes requirements that manufacturers of connected products and data processing service companies employ technical standards to permit interoperability and data portability. Accordingly, to facilitate access to and use of data by consumers and businesses, the proposals include provisions which enhance a user's right to share data with third parties (their portability right). It also contains specific interoperability provisions aim to facilitate switching between cloud and edge services. These measures aim to set the right framework conditions for customers to effectively switch between different providers of data-processing services and contribute to an overall framework for efficient data interoperability.

The data portability and interoperability provisions in the Data Act proposal, which primarily seek to facilitate switching, are targeted at data processing services, notably cloud and edge computing services, which provide the technological basis that makes data access and use possible.

A data processing service is defined under Regulation (EU) 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market with EEA relevance (Portability Regulation) as "*a digital service other than an online content service […], provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature" (Article 2(12)). Data processing services "should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other virtual or physical infrastructure, operating systems, software, including software development tools, storage, applications and services" (Recital (71)*).

### Data portability under the Data Act proposal

The Data Act proposal enhances a user's right to share their data with third parties. This is a result of the Commission's view that users of objects or devices generally believe that they should have full rights to the data they generate, but that these rights are often unclear and manufacturers do not always design their products in a way that allows users, both professionals and consumers, to take full advantage of the digital data they create. As such, a number of provisions under the Data Act proposal support the right to data portability, with a particular focus on data generated in the IoT environment. In relation to data processing services, the Data Act proposal also aims to enhance data portability as a means of promoting switching between cloud services providers, notably in such a way that ensures the customer enjoys "functional equivalence" (as defined under Article 2(14)) between services after switching provider.

The Data Act proposal provides for rights to access, use and share IoT-generated data which are essentially constructed around the concept of data portability established in respect to personal data under the GDPR. Such rights entail corresponding duties for the data holder to make such data available to the user or to third parties "*without undue delay, free of charge and, where applicable, continuously and in real-time*" (Articles 4 and 5, Data Act proposal). However, gatekeepers under the DMA are not an eligible third party under Article 5 Data Act proposal. In addition, the data portability provisions under the Data Act proposal will not apply to data generated by the use of products manufactured or related services provided by SMEs (Article 7(1)).

As regards data switching, providers of a data processing service are required to take specific measures to ensure that customers can switch to another data processing service, by removing commercial, technical, contractual and organisational obstacles which inhibit customers from porting their data, applications and other digital assets to another provider of data processing services (Article 23(1)(c), Data Act proposal). Article 26 of the Data Act proposal outlines the technical aspects of switching, differentiating between providers of certain infrastructure, such as servers, networks and the other virtual resources necessary to operate the infrastructure, but which do not provide access to the operating services and other providers of data processing services. The first category must ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service. The other providers must make

interfaces publicly available and free of charge, ensure compatibility with open interoperability specifications, or, lacking such specifications, export all relevant data in a structured, commonly used and machine-readable format.

### Interoperability under the Data Act proposal

The Data Act proposal defines interoperability as the "*ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions*" (*Article 2(19)*).

The Data Act proposal defines "functional equivalence" as "the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract" (*Article 2(14)*).

The Data Act proposal's Impact Assessment Report identified two main issues in relation to interoperability in the data economy which have not been addressed by existing instruments: lack of interoperability between cloud services and hurdles to effective switching between providers across the market (beyond gatekeepers) and lack of data interoperability. It highlighted not only that the scope of existing technical means for ensuring interoperability when porting data is unclear, but also that manufacturers generally do not offer interoperable formats and interfaces for standardised data exchange, which practically impacts the ability of consumers to exercise their right to data portability. As such, the interoperability provisions of the Data Act proposal largely support and enable the exercise of data portability. Additionally, the Commission noted that the fairness of cloud and edge services is threatened where users are inhibited in switching from one provider to another because of contractual, economic, and technical obstacles, an important part of which is a lack of interoperability, particularly with regard to Platform-as-a-service and Software-as-a-service services offered by a myriad of providers. Therefore, the interoperability provisions also aim to facilitate switching and prevent vendor lock-in.

The solutions the Data Act proposal intends to encourage consist of open interoperability specifications to enable a seamless multi-vendor cloud environment and standardisation and semantic interoperability, as well as common specifications (as defined under Article 2(15) therein) to be adopted by the Commission to enhance interoperability for the common European data spaces, application programming interfaces, cloud switching and smart contracts (see Recitals (76) and (79)).

Chapter VI of the Data Act proposal introduces minimum regulatory requirements imposed on providers of cloud, edge and other data processing services, to enable switching. In particular, Article 26 mandates that customers enjoy the same functional equivalence in the use of the new service after switching, in certain cases requiring data service providers to make open interfaces publicly available and free of charge, and in other case ensuring compatibility with open interoperability specifications or European standards for interoperability identified in the proposal. The Data Act proposal does not

mandate specific technical standards or interfaces; however, it requires services to be compatible with European standards or open interoperability specifications.

The provisions under Chapter VIII of the Data Act proposal set out the requirements for interoperability for operators of data processing service providers, operators of data spaces, and smart contracts for data sharing. Hence, businesses will have to take into account the provisions under Articles 28-30 of the Data Act proposal in order to allow the recipient to find, access and use the data.

The following sections will set out the competition concerns which have been identified around lack interoperability and data portability, how competition and privacy laws have tried to remedy such concerns and illustrate the potential impact the draft Data Act provisions may have in these areas. While the Data Act proposal and competition law seeks to address similar concerns arising from lack of interoperability and portability (that is, encouraging openness, switching, and reducing customer lock-in), the following analysis will assess the extent to which the Data Act proposal may change the status quo in these spheres or lead to any potential tensions.

## Competition: data portability and interoperability

In the competition sphere, interoperability and data portability have been identified as two key aspects which can promote multi-homing and switching, enabling new entrants to provide effective competition against incumbents and other large firms. According to the Commission's final report on Competition Policy for the Digital Era, portability of data refers to the ability of users to transfer the data that a platform has collected about them. In that report the Commission noted that interoperability is different to portability, and can take various forms, namely protocol interoperability, data interoperability, full protocol interoperability. **Protocol interoperability** is the form which has typically been considered under competition law, and refers to the ability of two services or products to interconnect, technically, with one another, while **data interoperability** is roughly equivalent to data portability but with a continuous, potentially real time, access to personal or machine user data. **Full protocol interoperability** refers to standards that allow substitute services to interoperate, for example, messaging systems (see Legal update, Commission publishes final report on competition policy for the digital era).

## Specific data-related concerns that EU competition law, competition policy, and recent competition law-inspired regulation seek to remedy

The OECD has observed that "*antitrust concerns related to the degradation of data portability and interoperability arise when artificial barriers to data flow are created, access to data that they might have otherwise legally accessed is foreclosed, and rivals' ability to compete is limited. Obstacles affecting access to private data may increase switching costs and lock-in effects, limit multi-homing and prevent users from enjoying the benefit of data*" (see Summary of Discussion of the Roundtable on Data Portability, Interoperability and Competition, June 2021). Importantly, interoperability undermines the networks effects associated with so-called "digital markets" and facilitates new entry and market contestability.

### Overcoming network effects and barriers to entry

As discussed above, network effects or externalities refer to a service's ability to improve its functionality as the number of users and data it is able to collect increases. As such, commentators have proposed mandating interoperability to overcome network effects and break the cycle it can create by concentrating large amounts of personal data, content and value (see Legal update, Digital Competition Expert Panel publishes its report). As reported in the Commission's impact assessment of the Digital Markets Act, digital rights' associations have pointed to lack of meaningful interoperability, as well as data access, as important barriers to entry in digital markets. Telecom operators also commented that to avoid lock-in effects for consumers, data portability which enables continued and far-reaching access possibilities is required, whereas the right to data portability in Article 20 of the GDPR is limited to specific cases and subject to specific legal bases for processing (see *Data portability*).

### Customer/vendor lock-in: preventing multi-homing and switching

The key benefit to interoperability and requiring platforms to interoperate with each other is in enhancing customer choice, rather than having the option of using only the service provided by the incumbent or largest firm. Data portability has similarly been cited by the former Commissioner for Competition, Joaquin Almunia, as going "to the heart of competition policy as in a healthy competitive environment consumers can switch from one provider to another by taking their own data with them." Recital 59 of the DMA articulates the concerns that arise from the vast amounts of data presumed to be collected by gatekeepers, and explains that the provision mandating data portability is necessary "*[t]o ensure that gatekeepers do not undermine the contestability of core platform services, or the innovation potential of the dynamic digital sector, by restricting switching or multi-homing*". Data portability is cited as particularly important for social networking sites and cloud computing services, where vast amounts of user-generated data are stored and may, therefore, present a barrier to switching or multi-homing. In relation to cloud computing services, the Commission has noted that the most usual type of practices observed include providers imposing obstacles to interoperability and data portability.

The Dutch NCA's recent market study into cloud services has also reported concerns around customer lock-in owing to "switching barriers", which include technical barriers to transporting data between cloud providers and poor interoperability preventing users from combining services from different providers (see ACM Market Study Cloud Services). The Commission's final report into IoT also found that "*interoperability among smart devices, voice assistants and consumer IoT services, is essential for the full deployment of functionalities that a consumer IoT ecosystem can offer to the user*", while interoperability between different brands enhances consumer choice and prevents lock-in to a single provider's products (see Legal update, European Commission publishes final report in consumer Internet of Things sector inquiry). While this is consistent with the Data Act proposal's specific objectives which include "*[f]acilitat[ing] switching between cloud and edge services – Access to competitive and interoperable data processing services is a precondition for a flourishing data economy, in which data can be shared easily within and across sectoral ecosystems*" (see *Explanatory memorandum*), customers may find value in, for example, the simplicity of using products and services from a single provider, and this may also lend itself to less "multi-homing" or switching, rather than lack of interoperability per se.

### Self-preferencing

Where an undertaking is vertically integrated, limiting interoperability for downstream customers can be considered exclusionary conduct (for example, Apple App Store; Apple Pay) which results in a preference for the dominant undertaking's competing product or service on that adjacent market. By limiting interoperability between applications and an operating system or mobile ecosystem, for example by restricting access to APIs, vertically integrated firms are able to engage in technical self-preferencing. Apple is currently being investigated for such practices, whereby it does not give access to its Near Field Communication chip to app developers, which Apple Pay uses and is necessary for digital wallet services and contactless communication (see Legal update, Commission sends statement of objections to Apple alleging abusive practices regarding Apple Pay). As described below, a competition law approach would currently require an analysis of this practice and potential remedy by a dominant undertaking under the refusal to supply case law and essential facilities doctrine of Article 102 of the TFEU.

### Examples of data-related practices involving interoperability and data potability that raise such competitive concerns

Firms may seek to prevent competition and reinforce their position on the market by limiting data portability and restricting key Application Programming Interfaces (APIs) that restrict interoperability. In its impact assessment for the Digital Markets Act, the Commission noted that unfair practices listed by respondents included "limited data portability and data access due to lack of interoperability (e.g., *APIs, limits to sharing customer data, restrictions to access key components, software or hardware), which creates obstacles for emerging competitors and also favours consumers lock-in. Several stakeholders refer to "walled-gardens", which allow to determine who can access the data uploaded by their end-users and on which terms and conditions*".

Device manufacturers and operating system providers prevent consumers from installing alternative app stores from which they can directly install applications into their mobile devices. For example, Apple restricts any app store other than its Apple App Store to be accessed or installed on its devices. The CMA has found that "*Apple earns substantial and increasing revenues from its App Store through commission on certain in-app payments and subscriptions, achieving higher gross profit margins than it makes on device sales*" (see Mobile ecosystems: Market Study Final Report). As such, Apple is incentivised to prevent the interoperability of competing app stores (which would reduce its potential for App Store derived commission) on its operating systems and devices. Prior to the DMA (or even now where such a company is not a gatekeeper) competition law seeks to remedy this behaviour as amounting to an abuse of a dominant position. While there is an established line of case law applying Article 102 TFEU to such refusals to grant access to inputs covered by IPRs, the threshold this has set means that a remedy enforcing the interoperability under this framework has scarcely been applied (see *Interoperability*).

Such potentially anti-competitive practices relating to data portability and interoperability have specifically been identified by the Commission in its final report on the IoT sector, where it noted that integration processes are largely determined by leading providers of proprietary voice assistants and operating systems, which can independently determine interoperability requirements through unilaterally governed terms and conditions,

technical requirements and certification processes, as well as imposing technical constraints (that is, limited APIs) and limiting functionality of third-party devices and services compared to their own (see Legal update, European Commission publishes final report in consumer Internet of Things sector inquiry). The Data Act proposal also recognises the importance of the proliferation of products connected to the IoT, raising concerns that when consumers buy a connected product (for example, a smart home appliance or smart industrial machinery) generating data, it is often not clear who can do what with the data. Moreover, it noted in the Impact Assessment Report for the Data Act that the market structure of IoT (as opposed to self-standing online services, including banking, insurance, food delivery, platforms providing daily services) suggests that the manufacturers hold an exclusive position over the data that is necessary for aftermarket services.

## How competition and privacy fields have attempted to remedy such concerns by enforcing interoperability and data portability

### Data portability

**Data portability: EU competition law and recent competition law-inspired regulation**

- **Competition law**. The competition case law and theories of harm that relate specifically to a user's right to data portability are not well established, and instead focus on interoperability and technical barriers implemented to impair data portability. Nevertheless, for the reasons set out above, data portability is a clear non-specific policy objective for the Commission (see Legal update, Commission publishes final report on competition policy for the digital era). That being said, the Italian NCA is currently investigating whether Google has abused its dominant position by hindering data portability rights and interoperability in sharing individuals' data with other platforms. The case follows a complaint filed by Weople, an app launched by Italian company Hoda, which provides users with a "digital vault" where they can port their personal data from third party accounts (including Google accounts) for data monetisation purposes. Weople anonymises user's personal data before sharing it with third parties. Advertisers then analyse the anonymised data provided to them by Weople, which subsequently identifies the best target users for the aforementioned third-party's advertisement, and sends it to the user. As consideration for the sharing of their personal data and the consent to receive the third-party's personalised advertisement, Weople pays the users monetary consideration.

The Italian NCA has observed that "Google's conduct could compress the right to portability of personal data, established by Article 20 of the GDPR, and could constrain the economic benefits that consumers can derive from their data" (see Press Release). It echoed the concerns around lack of interoperability and data portability, as well as their inherent complementarity, by stating "*the right to portability, if accompanied by effective interoperability mechanisms, can offer users the opportunity to achieve the maximum economic potential from the use of personal data, also through modes of exploitation that are different from those currently practiced by the dominant operator*".

- **DMA.** The Commission has noted that "*while the general criteria for creating duties to ensure data access - and possibly "data interoperability" (i.e., continuous data portability) - can be taken from Article 102 TFEU, ensuring frictionless data*

*interoperability on an ongoing basis will surpass the capacities of competition authorities*" (see Commission's final report on Competition Policy for the Digital Era). As such, to facilitate switching between different services and multi-homing, Article 6(9) of the DMA requires gatekeepers to ensure portability and provide free-of-charge tools to enable end users to port the data they generated on the gatekeeper's CPS, as well as providing such data to third parties where authorised by the end user. Notably, however, Article 6(9) does not define "authorised" or clearly set out the level of consent required for valid authorisation. While competition objectives may favour a less onerous threshold for valid authorisation so as to generate competition, the protection of privacy and the rights of individuals (as described above) may constrain this provision by requiring "freely given, specific, informed and unambiguous" consent mechanisms before personal data can be shared with third parties, in accordance with the requirements set out in the GDPR (see, for example, Articles 4(11) and 7(1)) and clarified by the EDPB's Guidelines no. 5/2020 on Consent.

Despite these attempts by both traditional competition law and DMA provisions, commentators have observed that data portability in itself may not be sufficient to keep data-driven markets contestable for new entrants and preventing consolidation. They cite the hybrid nature of data portability, which acts both as an instrument to empower individuals giving them control over their data (as envisaged by Article 20 of the GDPR), and to promote the free flow of data to stimulate the internal market, competition and innovation (as expressed through the provisions of the Data Act proposal). Accordingly, the various interests create inherent tensions which may prevent data portability "reaching its potential for stimulating data protection, competition and innovation" (see The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation, CPI Antitrust Chron. (Nov. 2020)).

**Data portability: Privacy perspective**

When data is personal data, the right of data portability, as outlined in the GDPR (Article 20), applies to any data subject in relation to potentially any personal data, that is, irrespective of any implications from a competition standpoint.

The GDPR constructs the right to data portability as follows: "*To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller [including directly, i.e., from one controller to another, where technically feasible]. Data controllers should be encouraged to develop interoperable formats that enable data portability*" (*Recital (68) and Article 20(1)-(2), GDPR*).

At the same time, the right to data portability "*should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible" (Recital (68), GDPR*).

Additionally, all other provisions of the GDPR apply, including those set out under Chapter III outlining data subject's rights, which include, among others, the rights to

receive complete and transparent information about the processing, right of access, rights to rectification and erasure, right to object (including to automated individual decision-making).

As outlined in the WP29 Guidelines of 13 April 2017 on the right to data portability, this right is in fact twofold, as it concerns the data subject's right to:

- **Receive personal data from the data controller:** The data subject has the right to receive a subset of the personal data concerning them processed by a controller. In this regard, data portability complements the right of access and results in data subjects being in a position to manage and reuse personal data themselves. As noted, the provision also requires that data be received in a structured, commonly used and machine-readable format.
- **Transmit (or obtain transmission of) personal data from one data controller to another data controller:** The data subject has the right not only to obtain and reuse, but also to transmit their personal data to another controller, preferably by having the personal data transmitted directly from one controller to the other, where technically feasible.

Notably, Article 20(1)(a)(b) of the GDPR limits the right to portability exclusively to processing activities that rely on consent or a contract as the lawful basis for the data processing and providing that such processing is carried out by automated means.

The WP29's Guidelines on the right to data portability consider that the right to portability covers "*data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity*". The EU legislator's decision to limit the right in the GDPR as per the above, however, may prevent data subjects from potentially maximising the value of their personal data, despite such data having inherent economic value (for example, in terms of allowing for the processing their personal data for marketing purposes based on the controller's legitimate interest). At the time of publication of this article, there is an ongoing debate as to whether and within what boundaries legitimate interest can be used to widen the scope of permitted processing activities. For instance, the EU Court of Justice is due to rule on a referral from the Amsterdam District Court to clarify whether legitimate interest can be used for commercial purposes under the GDPR (see CJEU Case C-621/22 Request for preliminary ruling).

The WP29's Guidelines further outline that the right to data portability may concern:

- Data actively and knowingly provided by the data subject (for example, mailing address, username, age).
- Observed data provided by the data subject by virtue of the use of the service or the device (for example, search history, traffic and location data, and any other raw data collected by the device, such as heartbeat or sleep pattern).
- Inferred data and derived data, that is, data created by the controller based on the (raw) data provided by the data subject or generated through an IoT device.

The Data Act proposal only applies to the first two categories above, further complicating the data portability framework, by requiring businesses and consumers to determine, on the one hand, whether the GDPR may apply to a given transaction based on the type of data being processed (that is, personal or non-personal) and, on the other hand, whether the Data Act proposal may also apply by differentiating between raw and inferred data (see Data portability).

In 2019, the Spanish DPA issued a resolution on the right to portability clarifying the scope of what the data ”provided” to the data controller refers to in the GDPR. The resolution follows a complaint filed by a user who exercised his right to portability to a telecommunications company and who was not satisfied with the data provided, since the telecommunications company only wanted to allow the portability of the data that the applicant had directly provided: name, surname, DNI, telephone, address, e-mail and bank details. The data subject claimed that he should have been provided with certain data listed in the privacy policy and resulting from the use or development of the service, such as products or services, consumption, traffic, visits to websites and location. The resolution found that the portability of the data was only partially carried out and that the data controller should have provided some of the additional data requested by the user. This decision extends the content of the right to portability to certain data resulting from the use of the service such as consumption, traffic and location, but without including data on visits to web pages. On the contrary, the resolution excludes the data referred to under Spanish law no. 25/2007 on data conservation for the purpose of investigating crimes from the scope of the rights to access and data portability pursuant to the GDPR.

Article 20 of the GDPR further requires data to be transferred in a “structured, commonly used and machine-readable format”. That is, the concept of data portability is based on the idea of interoperability as the desired outcome, which data controllers “*should be encouraged to develop*”. According to the above-referenced WP29 Guidelines, interoperability in the context of the GDPR stands for the “*ability of disparate and diverse organizations to interact towards mutually beneficial and agreed [on] common goals, involving the sharing of information and knowledge between the organizations, through the business processes they support, by means of the exchange of data between their respective ICT systems*”.

Referring again to the wording of Article 20(1) of the GDPR, the following minimum standards must therefore collectively be met:

- **Structuredness:** the specific form depends on the individual context and sector. Examples of structured data formats are database formats such as XML and Excel files.
- **Commonly Used:** consistent with the usual practices and conditions on the market, for example, CSV and JSON, subject to change according to further technical developments.
- **Machine readability:** under EU law, a machine-readable format means “*a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure*” (*Article 2(13), Directive (EU) 2019/1024 of 20 June 2019 on open data and the*

*re-use of public sector information (recast)*). A paper printout, for example, is not machine readable, nor is its electronic equivalent (including PDFs).

As noted above, a data subject may require that the above data is transmitted from one controller to another, "where technically feasible". The above-referenced WP29 Guidelines outline that technical feasibility should be assessed on a case-by-case basis, and Recital (68) of the GDPR clarifies that Article 20 GDPR should not be read in such a way as to create an obligation for controllers to adopt or maintain processing systems which are technically compatible. However, this only adds to the lack of clarity around data portability under the GDPR, as, in any case, controllers "*should be encouraged*" to develop interoperable formats that enable data portability.

Although Article 20 of the GDPR introduced the right to portability, it is not a standalone provision under EU law. Notably, it presents similarities with certain sector-specific data access regulations, especially in the digital content/services industries pursuant to Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (**Digital Content Directive**), although their objectives and coverage are different.

Article 16(4) of the Digital Content Directive obliges suppliers of digital content or services, when dealing with consumers, to make any content other than personal data available to them upon request, which was provided or created by the consumer when using the digital content or digital service supplied by the trader. This consumer right, however, does not apply in a variety of situations where the content is of little practical use to the customer (*Article 3*).

The Data Act proposal provides for two specific cases where the right to portability shall be ensured in accordance with the principle laid out in the GDPR. First, the by aiming to remove obstacles to switching between providers of data processing services:

- Article 23 requires that providers of a data processing service must ensure that their customers can switch to another data processing service which covers the same service type but is provided by someone else. Hence, providers must remove commercial, technical, contractual and organisational obstacles that prevent customers from enjoying their rights to terminate the agreement of the service, enter into an agreement (of the same type) with another provider, port their data, applications and other digital assets to another provider of processing services, and maintain "*functional equivalence*" of the service in the IT-environment of a different provider.
- Article 24 sets out certain minimum contractual terms that agreements with providers of a data processing service must contain, including clauses allowing the customer to switch to a third party's data processing service or to port data and weighing the provider to cooperate and complete the switch, "*where technically feasible*", within thirty days, providing an exhaustive list of the exportable data and application categories and a minimum period of data retrieval of at least thirty calendar days.

- Article 25 governs the charges that providers may apply for switching, outlining that following the entry into force of the Data Act and a transitional period, no charges for switching shall be applied to customers.
- Article 26 specifies technical aspects relating to switching the providers of processing services must adhere to, including in terms of functional equivalence, making open interfaces publicly available and free of charge or ensuring compatibility.

**Data portability: impact of the Data Act proposal on both competition and privacy**

Given that the Data Act proposal specifically seeks to enshrine and enhance a user's data portability right, this is an area where the Data Act proposal could impact the position from a competition perspective. Up until the DMA, competition enforcement and indeed EU competition law has been largely silent on enforcing this right. The Data Act proposal may therefore fill this potential enforcement gap. However, notably, the obligations on firms to provide consumers with access to data and to share this with third parties under Chapter II are largely limited to manufacturers of connected products (that is, IoT products) and related services (as the Commission found that is no compelling evidence of concerns relating to exclusive data use to extend new data access rights to all digital services), and Chapter VI, enforcing the right the portability of data by removing obstacles to customers porting their data, apply only to data processing services providers. As such, its scope and potential impact on firms may be limited. While the DMA represents a significant change with respect to data portability obligations, this of course will only apply to gatekeepers and their covered services (within the meaning of the DMA), and therefore those companies which are not designated but fall within the scope of the Data Act proposal will have to comply with the rights and obligations set out above.

The Data Act proposal may also help fill the enforcement gap in relation to privacy laws, considering that Article 20 of the GDPR limits the right to portability only to processing carried out by automated means and relying on consent or contract as lawful basis. The Data Act is meant to complement the rights and obligations set out under the GDPR and therefore may offer additional ground for customers to seek interoperability and portability of their personal data, albeit, as said, only in relation to IoT. Under the Data Act proposal, the scope of the right to data portability is broadened and includes any data generated by the use of a product or related service regardless of the nature or origin of the data (whether personal and non-personal, passively or actively provided) or, in relation to personal data, the legal basis for its acquisition under GDPR, with the only exception being derived or inferred data. The provisions facilitating switching between data processing services also appear to have been loosely inspired by the GDPR's portability rights.

**Interoperability**

Competition law has typically assessed such practices and consequently enforced interoperability under Article 102 of the TFEU. While there a number of such ongoing investigations into the practices identified above, competition law's ability to directly intervene to mandate interoperability has been limited to where the restriction on interoperability amounts to a refusal to grant access to IPRs (for example, interoperable interface information between the undertaking's platform / software and its competitors

downstream). *Bronner* line of case law (see Data access: EU competition law and recent competition law-inspired regulation, *above*) has been applied such that a duty to grant protocol interoperability has been imposed as a remedy in certain leveraging cases, for example, the Microsoft cases.

From a privacy angle, interoperability is a necessary basis to ensure that data subjects can enjoy their right to data portability, but should be aligned in accordance with the core transparency and data minimisation principles.

### Interoperability: EU competition law and recent competition law-inspired regulation

**Competition law: Protocol interoperability** - Microsoft. In the Microsoft cases (Commission decision of 24 May 2004 in Case C-3/37792 - *Microsoft*, Commission decision of 16 December 2009 in Case 39530 - *Microsoft (Tying*) and General Court judgment of 17 September 2007 in Case T-201/04 - *Microsoft v Commission*), the Commission and European Courts found that Microsoft had refused to supply interoperability information to competitors on the downstream market (leveraging its dominance in operating systems) amounting to an abuse of its dominant position. It was shown that: the refusal was likely to eliminate all competition on downstream market, access was indispensable to carrying on the downstream competitor's business, meaning that there is no actual or potential substitute available, the refusal supressed the emergence of a new product (specifically as this threatened "follow on" innovation), and there was no objective justification. Accordingly, Microsoft was required to provide such interoperability information with non-Microsoft work group services to achieve full interoperability with Windows PCs and servers, on reasonable and non-discriminatory terms (see Practice note, Competition regime: Article 102: Microsoft/W2000).

**The DMA.** Taking the view that interoperability is essential for effective competition and market contestability, the DMA includes new and far-reaching obligations related to interoperability. Gatekeepers once designated will need to provide interoperability between, under Article 6(4), their operating systems and third-party software applications and app stores, and under Article 6(7), their hardware, software and operating systems and third-party software and hardware providers. To address interoperability between messaging services, under Article 7, subject to conditions, gatekeeper messaging services must interoperate with competing messaging services for basic functions such as text messaging, voice and video calls and sharing files. Recital 57 explains that the preventing such interoperability "*significantly undermine*[s] *innovation by such alternative providers, as well as choice for end users*" and that therefore *"the aim of the obligations is to allow competing third parties to interconnect through interfaces or similar solutions to the respective features as effectively as the gatekeeper's own services or hardware".* Given that access to interoperability information has been carefully analysed under the scrutiny of the "essential facilities" doctrine above, mandating such access under the DMA may lead to unintended consequences, potentially hampering innovation and investment.

**Interoperability: privacy law**

From a privacy angle, interoperability is a necessary basis to ensure that data subjects can enjoy their right to data portability, although interoperability cannot give rise to the access or use of any data via another information system, or give access to more data than is needed, for instance, as noted by the European Data Protection Supervisor (EDPS), in cases where large-scale datasets have been created at an EU level that ensure communication and exchange of information for specific purposes (see EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems).

**Interoperability: impact of the Data Act proposal on both competition and privacy**

The Data Act proposal would have the greatest impact on cloud and data processing service providers' facilitation of interoperability as compared with the traditional competition law approach. As mentioned above, Chapter VIII of the Data Act proposal provides essential requirements regarding interoperability that operators of data spaces and data processing service providers must comply with, and Chapter VI introduces minimum regulatory requirements of contractual, commercial and technical nature that providers of cloud, edge and other data processing services must comply with, including ensuring that customers enjoy technical functional equivalence when switching between data processing service providers. The scope of these functional equivalence obligations and the extent to which they will mandate interoperability for cloud and edge service providers is currently unclear but potentially far reaching. As drafted in the Data Act proposal in relation to "functional equivalence" requirements is likely to significantly impede competition in the markets in which it is applied, as this will eliminate product differentiation and reduce incentives to innovate. This is likely to lead to a race to the bottom as data processing service providers are likely to be able to compete only on price. This would run counter to and undermine the objectives of the Data Act and competition law and policy. Imposing "functional equivalence" requirements is likely to significantly impede competition in the markets in which it is applied, as this will eliminate product differentiation and reduce incentives to innovate.

Where a gatekeeper's service is designated as a "covered service" under the DMA, the obligations under the Data Act may make little difference to such gatekeeper. However, as the provisions of the Data Act proposal currently apply to all data space operators and cloud and data processing services providers, these provisions may impact a larger number of firms. Notably, the current proposal does not mandate specific technical standards or interfaces, nor does it force firms to share interoperability information or APIs with other companies, which could represent a significant shift away from the existing approach to enforcing interoperability under traditional competition law. In this context, the DMA certainly goes further than the Data Act proposal and represents a far greater change to traditional competition law's approach to interoperability with respect to gatekeepers to whom it applies. This could reflect the focus of interoperability under the Data Act proposal as a means to facilitate switching and ensuring the portability of data to achieve this.

Consistently, from a privacy perspective, interoperability provisions under the Data Act proposal may play an important role in support of data subjects aiming to enforce their right to data portability. As said, interoperability is not in itself a purely privacy right,

however, by ensuring that a user is in a position to switch from one platform to another, the Data Act proposal also reinforces data subjects' rights to obtain portability of their personal data in that context, contributing to the development of practices and protocols that, in a forward-looking perspective, may then be used for portability purposes more widely and may help further clarify the scope and boundaries of the right to data portability. This is of particular importance in the context of the current debate over the right to portability, which focuses, among others, on the data subject's possibility to rely on portability to monetise their own personal data. Recently, the matter reached the EDPB following a referral from the Italian DPA in relation to the Weople case, in relation to the recent Italian NCA investigation concerning allegations that Google hindered its users' right to portability towards Weople (see Interoperability, *above*). The scrutiny of the Italian DPA concerns the very nature of Weople's data intermediation business: In its referral to the EDPB, the Italian DPA sought clarification in relation to two key issues, which may be relevant throughout the entire EU: the "*merchantability*" of the data and the problem of exercising the right to data portability by delegated powers (that is, risking possible duplication of the databases being "ported").

# DATA SHARING AND DATA POOLS

## Data sharing arrangements

Data sharing and pooling arrangements can offer new opportunities for data monetisation in the form of data sets, products and services, creating new revenue streams, increasing the marketable base of customers, helping with new industry and market insights, and enhancing AI capabilities and tools. Notably, sharing and pooling arrangements between multiple organisations or entities enable individual data holders to create additional value and insights that they would not be able to create on their own. This opens the door to new opportunities for collaboration without merging (see OECD (2020), Enhancing data sharing, access and re-use).

It is likely that the provisions on access to data, interoperability and portability contained in the Data Act proposal, analysed in the previous sections of this article, would facilitate data pooling and sharing arrangements within the EU, particularly in the following forms:

- Data pools. Though there is no legal definition of data pooling or data pools, in general terms, data pooling refers to the aggregation and combination of datasets acquired from different sources.
- Data trusts. Data trust are built around a concept of pooled or shared resources subject to a collective understanding around access or use (see Scassa, Teresa. (2020). Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto. Technology and Regulation). Compared to data pools, data trusts introduce an element of collective management of individual rights to data access and use, in the form of a third party, independent from both data holders and data users, who makes decisions on their behalf regarding access to and use of the data in the data pool. Essentially, data trusts introduce an element of data stewardship to sharing and pooling arrangements, whereby an independent third party decide who has access to the data, under what conditions, and to whose benefit.

Although incubated in AI, data trusts have broader potential across the field of data science and, more generally, in helping organisations manage data sharing responsibilities in relation to:

- personal data under the GDPR;
- non-personal data;
- cloud / information security and governance; and
- AI deployment / ethics (see *Article, Data trusts: on the cusp of widespread adoption*).

Data trusts have the potential to increase data access and sharing, with social and economic benefits to society, whilst ensuring rights and interests such as privacy and corporate confidentiality are protected. Governments and stakeholders are exploring potential uses of data trusts through a wide variety of pilot projects.

In 2017 Sidewalk Labs (an Alphabet subsidiary) announced plans for a "smart city" development on the waterfront of Toronto, Canada, with the ambition of creating a carbon-positive city. The creation of an Urban Data Trust was central to the project in order to balance the diverse interests in the data that might be collected in the development. The failure of the Urban Data Trust project has offered insight into some of the challenges that are central to data governance for data sharing (see *Scassa, Teresa. (2020)*).

More recently, the Open Data Institute (ODI), in partnership with the UK Office for AI, are running data trusts pilots to examine the potential of data trusts to:

- make video and audio captured in wildlife settings by researchers and conservationists more accessible, ultimately aiming to use the data to reduce illegal trade of wildlife;
- apply to food supply chain data with the aim of reducing food waste by improving the ability of retailers and manufacturers to track and measure food waste within supply chains; and
- how energy consumption data collected by sensors and devices in buildings, data relating to parking space occupancy and to the availability of charging bays for electric vehicles might be made available through a data trust.

Following public reluctance to opt into the data pooling project developed by NHS Digital to collect patients' primary care (GP) to be used in a non-identifying form for health research and service planning purposes, a group of researchers based at the University of Manchester is piloting a data trust model (the General Practice Data Trust), funded by the Data Trusts Initiative, to find out why people opted out of sharing their GP data and to explore whether a data trust would provide a more widely accepted method of sharing GP data.

The UK Food Standards Agency is looking into the "*potential of automated and autonomous systems, such as fruit-picking robots and smart production lines, of digital technologies such as the Internet of Things and artificial intelligence*", considering that "*[r]eliable information from across the sector about, for example, allergen data, product authenticity, provenance, nutrition and sustainability, will help serve public needs and consumer expectations. For food suppliers, it could speed up processes and save money. For the Food Standards Agency (FSA) and the UK government, a move towards easier data sharing could enable a more targeted, risk-based approach to inspections. It could also speed up information exchange along a chain in urgent situations such as food recalls and tracing incidents*" (see Food Data Trust: A framework for information sharing).

## The Data Act: data sharing and pooling

Companies are sitting on huge data reserves in the form of records, stocks, sales, and clients which when pooled together can translate into a new kind of competitive advantage. Personal data is just a fraction of existing data. The benefits of data sharing

and pooling arrangements for businesses and for the European market as a whole have guaranteed data pools a place in the EU data strategy. Moreover, according to the Commission, "*infrastructures should support the creation of European data pools enabling Big Data analytics and machine learning, in a manner compliant with data protection legislation and competition law, allowing the emergence of data-driven ecosystems*" (see Commission on the European strategy for data).

Though data pools are not yet covered by EU legislation, the Data Act proposal is the latest piece of the EU data strategy puzzle that is likely to indirectly facilitate data sharing and pooling arrangements. Such arrangements would fall within the scope of the Data Act proposal insofar as the data is "*generated by the use of a product or related service*", that is, by an IoT device, and made available to the user of that product or service, by data holders to data recipients or by data holders to public sector bodies or European institutions, agencies or bodies (*Article 1, Data Act proposal*). IoT devices could be a useful tool for pooling as they are capable of generating large amounts of data which can be fed into a data pool. Therefore, in regulating data generated by IoT devices and related services, the Data Act proposal would also indirectly contribute to creating a legal framework for data pools.

## Competition law: potential competition concerns which may arise from data pools and data sharing arrangements

EU competition law places restrictions on the exchange of commercially sensitive information (CSI) between competitors under Article 101 of the TFEU. Data pools and sharing arrangements may give rise to competition concerns in this context, or more indeed more broadly. The Commission specifically considered data sharing arrangements, and "data pools", which require some reciprocity of sharing, in its final report on Competition Policy for the Digital Era and commented that "*[t]he competition law assessment will necessarily depend, inter alia, on the type of data shared, the precise form of a data sharing arrangement or data pool as well as on the market position of the relevant parties. So far, the issue is a relatively new and under-researched topic in competition law*". It observed that data sharing and pooling arrangements are often pro-competitive as they enable firms to develop new or better products given the pooling of the same or complementary data. For these reasons, the assessment of data sharing and pooling arrangements should start with a recognition of the significant efficiencies they can produce (and such efficiencies were considered in CJEU Case C238/05 Asnef-Equifax and Administración del Estado [2006] ECR I11125, see Legal update, ECJ ruling on information exchanges between credit institutions). Despite these benefits, it also noted that data sharing and pooling may give rise to various competition concerns.

### Exchange of CSI and collusive outcomes

Data sharing arrangements and pools may include the sharing of CSI between competitors. While recognising that the exchange of information between companies is a common feature of many competitive markets and often has a legitimate purpose, competition concerns arise where these exchanges include CSI which artificially increases transparency and facilitates coordination and alignment of companies' competitive behaviour.

### Restricting access and anti-competitive foreclosure

Concerns may arise where competitors are denied access to such data pools (or only granted access on less-favourable terms) leading to anti-competitive foreclosure from the market. Data pools, particularly when covering a large part of the market, may yield an important competitive advantage in serving the market. The Commission's Guidelines on the applicability of Article 101 of the TFEU to horizontal co-operation agreements (OJ 2011 C11/1) (Horizontal Guidelines) note that information sharing may lead to anti-competitive foreclosure by placing unaffiliated competitors at a significant competitive disadvantage as compared to those affiliated with the exchange system. The Commission is set to adopt new guidelines on horizontal co-operation agreements later this year. The draft revised Guidelines on the applicability of Article 101 of the TFEU to horizontal co-operation agreements highlight in relation to data pools that "[w]*hen the data shared represents a valuable asset to compete in the market, competitors who are denied access (or granted access on less favourable terms only) might be foreclosed from the market*".

### Discouraging differentiation in data collection

Competition concerns may also arise when data pools impact the incentive to engage in or improve independent data collection which may compromise competition. This may give rise to greater concerns where data is a significant input into the parties' product and/or when inferred data is pooled.

### Continued access to data format standards

The Commission has highlighted that where a data pool's format standard is proprietary and a FRAND duty for access is imposed on the standard owner, it should not be able to increase the price of access to the pool over time as its importance increases. As such, concerns arise around enforcing ongoing use of such data on FRAND terms, as well as providing initial access.

## Privacy law: potential privacy concerns which may arise from data pools and data sharing arrangements

From a privacy perspective, the underlying concern behind any data sharing or pooling arrangement is that such arrangement inevitably entails a potential loss of control over the data itself. The tension between data sharing and protection of privacy is especially evident in the case of data pools, as large-scale data aggregation and sharing by way of data pools seems at odds with individuals' fundamental rights to privacy and data protection.

As regards data trusts, just like other types of trusts, the trustee has to act in the best interest of beneficiaries when exercising rights and making decisions on their behalf. From a privacy angle, declaring consent and invoking the rights of access, erasure, rectification and portability (*Articles 15 et seq., GDPR*) on behalf of data subjects fall within this notion. It should be noted however that the crucial question, that is, whether it is permissible under the GDPR for data subjects to delegate these decisions to third-party fiduciaries is far from being a settled one (see L. von Ditfurth, G. Lienemann, The Data Governance Act: Promoting or Restricting Data Intermediaries?, CRNI 2022, vol. 23(4)).

However, the potential risks associated with data sharing should be balanced against the risk of not realising the value of data. From a business perspective, the cost of risk mitigation may be comparatively small if the potential benefits consist in fresh commercial insights, efficiency savings or a new product or service in a competitive market. It has also been suggested that a stewardship model for data sharing is capable of overcoming the structural issues with privacy models based around consent, such as the GDPR, which are becoming more apparent with the emergence of large-scale data pooling and AI.

### Legal basis for data pooling

Data processing within the meaning of the GDPR includes sharing and pooling given the broad definition of 'processing' provided by Article 4(2) of the GDPR. Where the data being pooled contains personal data, the GDPR places substantial constraints on the processing of such data. Firstly, personal data processing is forbidden unless justified by any of the legal bases for processing outlined under Article 6 of the GDPR. Even where such legal basis is provided, the GDPR sets out additional compliance requirements for the processing of personal data, including in terms of record keeping and reporting, data transfers within and outside the EU, as well as differentiating special categories of personal data. Implementing such requirements may be tricky in a data pool context.

The Data Act proposal does not create an additional legal basis under the GDPR that could allow "*the data holder to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service" (Recital (24), Data Act proposal*). Therefore, the GDPR remains the only legislative act that provides the legal bases for personal data processing.

As regards non-personal data, where the manufacturer of the product is also the data holder, the basis for the manufacturer to use such data should be a contractual agreement between the manufacturer and the user. The Data Act proposal requires the data holder to enter into a contractual agreement with the user of the product (*Recital (24), Data Act proposal*). Thus, two legal bases, one under the GDPR and another under the Data Act proposal, may be required where a data pool is comprised of both personal and non-personal data.

### Purpose limitation

Users are expected be aware of the purposes their data is used for. However, identifying the purpose of data processing is difficult (if not impossible) in a data pooling context, where data is collected at a large scale to potentially create a "big data" pool, with the idea that new uses for such data may emerge, for example, the development of new technologies and AI. This is especially apparent in instances where the data is collected with the consent of the user; a likely scenario considering the requirement for a contractual agreement in order for a data holder to use non-personal data generated by the use of an IoT product or related service, as provided in the Data Act proposal.

Pursuant to Article 4(6) of the Data Act proposal, *"The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active"*.

Further, consent obtained at the time the data was initially collected may not be applicable to the purposes such data is subsequently used for in the context of a data pool. Ensuring GDPR compliance in such cases places unrealistic demands on data holders, who would need to ensure that any subsequent purposes the data is processed for are compatible with the initial purpose and the data is only used for purposes for which the data subjects could reasonably believe their data may be used for. Data pools therefore risk rendering privacy models based on purpose limitation obsolete.

### Shifting privacy compliance responsibilities to users

Data subjects' control of their data is a central issue in academic and policy debates related to data governance (see Botero Arcila, Beatriz and Groza, Teodora (2022), Comments to the Data Act from the Law and Technology Group of Sciences Po Law School, p. 2). By regulating data sharing, the Data Act proposal aims to enhance users' control of their own data. However, it has been noted that the Data Act proposal relies excessively on the idea of privacy self-management. The Data Act proposal requires users to request access to the data generated by their use of a product or related service and to share such data with third parties (*Articles 4 and 5, Data Act proposal*). A framework based on privacy self-management does not provide individuals with meaningful control over their data. First, privacy self-management is undermined by empirical and social science research which demonstrates that there are cognitive factors that impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to processing of their data. Second, there are too many entities engaging in data processing to make it feasible for individuals to manage their privacy separately with each entity. Both factors are particularly relevant in the context of data sharing and pooling arrangements, where the aggregation of data from different sources and time periods makes it virtually impossible for individuals to weigh the costs and benefits of sharing their data without an understanding of the potential downstream uses (see Solove, Daniel J. Introduction: privacy self-management and the consent dilemma. Harvard Law Review (2013), 126 (7)).

## How competition and privacy laws have attempted to ensure responsible data sharing and pooling and the potential impact of the Data Act in these areas

It is essential for data holders to ensure legal compliance prior to sharing data. Existing privacy and data protection laws demand a risk-based approach to data sharing.

### Data sharing arrangements and data pools: competition law remedies

Competition law typically relies on Article 101 of the TFEU to remedy and address the concerns which have been identified as potentially arising from information and data sharing. It should be reiterated, however, that the issues which can arise specifically in relation to data sharing arrangements and data pools are a "*relatively new and under-researched topic in competition law*" (see *Commission's Competition policy for the digital era*).

### Anti-competitive exchanges of competitively sensitive information (CSI)

In light of the collusive concerns identified in Exchange of CSI and collusive outcomes, certain exchanges of CSI (particularly in relation to price) may constitute a restriction "by object" under Article 101(1) of the TFEU where they favour collusive outcomes, while others may amount to a restriction "by effect" where competition is limited, for example, by price, quality or innovation, as a result of such exchanges aligning competitors' behaviour in the market (see Practice note, Information exchange and EU competition law). The Commission's Horizontal Guidelines set out the general principles on the competitive assessment of information exchanges between companies active on the same market and set out the various considerations which will be taken into account when considering a potential infringement.

### Restricting and enforcing access to competitors

Where these pools contribute to market power, competition law might be expected to impose a duty on dominant undertakings with access to such pools to grant access to competitors under Article 102 TFEU. However, in light of the difficulties in establishing indispensability where such datasets can be replicated, the successful application of Article 102 of the TFEU to data pools is unclear. Alternatively, and more commonly, restrictions on access to data pools which lead to anti-competitive foreclosure from the market have been found to infringe Article 101 of the TFEU.

On 18 June 2021, the Commission sent Insurance Ireland (an association of companies active in the insurance sector in Ireland which covers over 90% of the Irish motor vehicle insurance market), a statement of objections alleging an infringement of Article 101 of the TFEU on the basis that it had arbitrarily delayed or *de facto* denied companies with a legitimate interest in joining, access to its Insurance Link information exchange system (*Case AT.40511 - Insurance Ireland*). This contained important data allowing motor vehicle insurers to better assess customers' risk profiles, and consequently to price insurance policies for motor vehicles, and the Commission alleged that by restricting access, Insurance Ireland placed these companies at a competitive disadvantage vis-à-vis members with access to the platform (see Legal update, Commission sends statement of objections to Insurance Ireland for restricting access to Insurance Link data sharing platform). In September 2022, it accepted commitments from Insurance Ireland whereby it must ensure FRAND access

to its Insurance Link information exchange system, to overcome the anticompetitive foreclosure concerns which may arise from such data pooling arrangements (see Legal update, Insurance Ireland: Commission accepts commitments).

As competition law can be used in this way as a mechanism to expand the sharing of information more widely, this can exacerbate the tension with the protection of privacy. The impact of this may depend on the extent to which the information shared constitutes personal data, however in such cases the principles and application of the GDPR must be considered and may arguably constrain the ways in which competition law can enforce access.

### Potential exploitative abuses in relation to FRAND access

The Commission has suggested that there may be times where the granting of access to data on non-FRAND terms may result in an exploitative abuse under EU competition law. It has indicated that "*where there is a FRAND or similar duty and the pool's data format standard is proprietary, the standard owner should not be able to raise its fees over time as the pool becomes more important in the market (by analogy to "patent ambushes")*" (see *Commission's final report on Competition Policy for the Digital Era*). As such, the FRAND duty should apply to continuing use of the data pool.

## Data pools and sharing arrangements: impact of the Data Act and Data Governance Act

### Data pools and sharing arrangements: competition law

Recital (88) of the Data Act proposal highlights that it "*should not affect the application of the rules of competition, and in particular Articles 101 and 102* [of the TFEU]". As such, this would suggest that the data sharing provisions of the Data Act proposal do not envisage the creation of data pools or sharing agreements which could constitute anti-competitive sharing of CSI under Article 101. Separately, the Commission's draft revised Guidelines on the applicability of Article 101 of the TFEU to horizontal co-operation agreements do not cover data sharing initiatives under the Data Act proposal specifically which leads to uncertainty as to how these will be treated under Article 101.

### Data pools and sharing arrangements: privacy law

#### Impact of the Data Act proposal

It has been suggested that there are larger social values behind protecting privacy, and therefore the costs and benefits of data sharing are more appropriately addressed cumulatively and holistically, as opposed to merely at the individual level, as individuals' decisions about their own privacy affect society, not just themselves (see *Solove, Daniel J. (2013)*). A possible solution may be moving away from the privacy self-management model and enabling a third party acting as a data steward to manage data on behalf of users once they have received a clear mandate to operate and after-market service (see *Botero Arcila, Beatriz and Groza, Teodora (2022)*). Such a solution would be consistent with the Data Act proposal, which provides for users' data to be shared between the data holder and data recipient on the basis of an agreement which users themselves are not a party to (*Article 8, Data Act proposal*).

The data sharing rules under the Data Act proposal echo the minimisation principle set out by the GDPR (the latter applicable where personal data is concerned). In order to be able to access data generated from IoT devices, as well as to share such data with third parties, the user shall not be required to provide any information beyond what is necessary to verify the quality as a user. By way of example:

- **Right of users to access and use data generated by the use of products or related services.** Article 4(2) of the Data Act proposal prevents the data holder shall from requiring the user to provide any information beyond what is necessary to verify their quality as a user, as well as keeping any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.
- **Right to share data with third parties.** Article 5(3) of the Data Act proposal ensures that the user or third party is not required to provide any information beyond what is necessary to verify their quality as user or as third party, and the data holder does not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.

**Impact of the Data Governance Act**

By clarifying *who* can create value from data and under which conditions, the Data Act proposal intends to supplement another key pillar in the European strategy for data, the Data Governance Act (*Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (OJ 2022 L 152/1)*), which focuses on creating the *processes and structures* to facilitate data reuse and sharing, by ensuring that "*data intermediaries […] function as trustworthy organisers of data sharing or pooling within the common European data spaces*" (see Commission's overview of the Data Governance Act). The Data Governance Act entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from September 2023.

Similarly to the Data Act proposal, the Data Governance Act aims to enable a competitive environment for data sharing, whilst increasing the trust and control of data holders, data subjects and data users in data intermediation services. encourage the use of data that are made available voluntarily by individuals or companies for purposes of general interest, such as benefitting healthcare, combating climate change, improving mobility, compiling official statistics, improving public services and supporting scientific research.

**Data sharing and pooling.** On a regulatory level, the Data Governance Act will affect data sharing and pooling by providing a framework for re-use of certain categories of public sector data, in which third party rights exist (Chapter II). In particular, Article 3 deals with access to certain protected data (including under privacy law) by public bodies, which may be understood to include data stored with a trustee or mediated by the latter.

The Data Governance Act proposes a two-tier governance structure: a governance entity for each data space and an overall governance organisation concerned with common aspects of data space interoperability and data sovereignty which will define the roles within a data space (for example, data provider and data consumer), as well as the rules all actors have to abide by (see Opendei, Design principles for data spaces, 2021).

Pursuant to the Data Governance Act, a data intermediary is the general term for a party (for example, a broker, marketplace operator or facilitator) that organises the sharing and exchange of data between actors. With regard to data intermediaries, regulating data sharing services and control over access to data (Chapter III). According to the Data Governance Act, a key element to achieving this is ensuring "*the neutrality of data intermediation services providers with regard to the data exchanged between data holders or data subjects and data users*" (*Recital (33)*). The Data Governance Act adopts the purpose limitation principle in respect to data intermediation services providers, which can act only as intermediaries in the transactions, refraining from using the data exchanged for any other purpose (*Recital (33)*). Such principle, combined with the neutrality rule outlined above, indicates data trusts as a potential solution to the issues arising from data pooling, relating to purpose limitation, as well as protecting both data holders' and users' interests in respect to data access and use and, in doing so, complementing the Data Act proposal (where personal and non-personal data is concerned) and the GDPR (where personal data is concerned). It follows that the role of a data intermediation service within the meaning of the Data Governance Act could be carried out by a data trust.

**Data altruism.** The Data Governance Act creates a legal framework for data altruism with the aim of establishing trust among data holders to voluntarily share their data (*Recital (36)*), with the aim of facilitating the emergence of data sets in the EU large enough to enable data analytics and machine learning (*Recital (35)*). A register of recognised data altruistic organisations should be kept at national and EU level (*Article 15*) and organisations should be able to collect data directly from data subjects, as well as process data collected by third parties (*Recital (38)*).

Companies seeking to support purposes of general interest by making available relevant data would be able to register as recognised data altruism organisations. Registration would be valid across the EU, facilitating cross-border data use within the EU and the emergence of data pools covering several member states. Recognised data altruism organisations would be able to collect relevant data directly from natural and legal persons, or to process data collected by others. Typically, data altruism would rely on the consent of data subjects in accordance with the GDPR. Individuals and companies participating in these activities would consent to specific purposes of data processing but could also consent to data processing in certain areas of research or parts of research projects (see Article, Data Governance Regulation: the wave of regulatory and competition reform begins).

Under Article 2(11) of the Data Governance Act, a **data intermediation service** means "*a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data*".

*However, the same provision sets out "at least" the following exclusions: "(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users; (b) services that focus on the intermediation of copyright-protected content; (c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things; (d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships"*.

Moreover, the Data Governance Act provides for a definition of data altruism, which is central to the concept of a data trust, in the following terms: "*the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward [...], such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest" (Article 2(16)*).

# FUTURE REGULATORY APPROACH TO DATA

## Assessing the types of data being used

Businesses' obligations to comply with the GDPR and the Data Act proposal, when it comes into force, will have several practical implications. In particular, in situations where the Data Act proposal applies, businesses will need to identify whether the data affected can also be classified as personal data and, if so, if the GDPR or any other data protection regulations additionally apply and must be complied with.

This identification exercise will not always be easy:

- **Difficulties with the concept of personal data.** Classifying data as "personal" data is not always straightforward as such classification may at times depend on the context, the purpose for which the date is being processed or the state of the art, among other factors. Data could also be considered "non-personal" on the date that it is processed, but subsequently become "personal".
- **Anonymisation vs. pseudonymisation**. Data is considered to be anonymised when it cannot be associated with a particular individual, whereas (personal) data is considered to be pseudonymised when it cannot be attributed to a data subject without the use of additional information. Anonymised data sets do not fall within the scope of application of the GDPR. However, pseudonymised data sets are subject to data protection regulations.
- **Mixed data sets.** In practice, a data set is likely to contain both personal data (subject to the GDPR or other applicable regulations) and non-personal data.

In any of the above three scenarios, businesses are likely to be inclined to choose the most conservative position: treat the information as personal data and safeguard both the data subject (owner of the data) and the entity processing it. Similarly, in the case of data sets in which personal data is mixed with non-personal data, if it is not possible to separate both types of information, prudence dictates that the entire data set (including non-personal data) should be subject to the principles and obligations of the GDPR.

In light of the above, a careful assessment of whether a business purpose could still be achieved if the exchange of personal data was dispensed with altogether, or if the data to be shared was anonymised in advance, would be beneficial from both a privacy and competition law perspective.

## Data protection impact assessments (DPIAs)

Data pools and data trusts typically require the processing of high volumes of data and are therefore likely to represent a high risk to the rights and freedoms of natural persons, thus requiring a DPIA as set out in the GDPR. Pursuant to Article 35 of the GDPR, DPIAs are mandatory where the data processing entails any of the following:

- A systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, used to make decisions legally or otherwise significantly affecting natural persons.
- Large scale processing of any of the categories of personal data listed under Articles 9 and 10 of the GDPR.
- Systematic monitoring of a publicly accessible area on a large scale.

Existing examples of data pools and data trusts suggest that, more often than not, such data sharing arrangements would fall in at least one of the abovementioned categories; even where they do not (for instance, because the data being pooled is not personal data in the sense of the GDPR), from a data protection compliance perspective DPIAs are nonetheless best practice (see Data Pitch, Data Sharing Toolkit, p. 13).

## Data stewardship and data trusts

An alternative to the privacy self-management model is the creation of a data trust, whereby an authorised third party acting as data steward would manage pooled data on data subjects' behalf. Data trusts make sharing of data possible while still respecting the varying, and potentially contrasting, legal interests of its members. There are several potential legal structures that can be used to set up a data trust: from a traditional legal trust to a contractual framework model (see Data trusts: legal and governance considerations (2019)).

Where a mix of personal and non-personal data is concerned, it may be useful to set up different groups of data pools with different access rules to ensure both GDPR and Data Act proposal compliance (see Bjorn Lundqvist, Data Collaboration, Pooling and Hoarding under Competition Law, 2018, p. 9). Moreover, through a data sharing agreement and appropriate technical measures, a data trust could hide any data considered sensitive from everyone except those in the compliance role (see Wu, D, Verhulst, S, Pentland, A, Avila, T, Finch, K and Gupta, A (2021) How data governance technologies can democratize data sharing for community well-being. Data & Policy 3, E14). By way of a data trust, users would only need to enter into a single data use agreement with the data trust, rather than negotiating individual agreements with each data holder. Start-ups and small and medium enterprises who lack the experience and expertise to negotiate appropriate data sharing agreements would also benefit from being able to rely on the data steward's expertise.

## A combined competition and privacy compliance system

As a consequence of significant overlap between competition and privacy law, compliance requirements relating to both branches of law are becoming ever more intertwined, as confirmed in the recent opinion of Advocate General Rantos in the case involving Meta Platforms Inc (Meta) and the German NCA, delivered on 20 September 2022 (AG Rantos Opinion in CJEU Case C-252/21, Meta Platforms Inc. v Bundeskartellamt). Meta's alleged practice of leveraging interoperability capabilities to access and pool user-related data by collecting user and device-related data from other services belonging to the Meta group, including Instagram and Whatsapp, as well as from third-party websites and apps via integrated interfaces or cookies and linking such

data with the user's Facebook account and subsequently using (that is, processing) it. In doing so, Meta caught the eye of the German NCA, raising concerns relating to, on the one hand, potential abuse of dominant position and, on the other hand, potential non-compliance with the provisions of the GDPR. Meta appealed against the NCA's decision to the Higher Regional Court of Düsseldorf, which in turn asked the EU Court of Justice whether NCAs are entitled to assess the compliance of data processing with the GDPR. The Advocate General concluded that an NCA may incidentally examine GDPR compliance and, in doing so, should cooperate with data protection authorities (DPAs), including by taking account of any related decision or investigation of a DPA.

The Meta case is expected to be a defining point in consolidating the view that the use (that is, processing) of users' data for commercial purposes falls within the scope of both competition and privacy law, already expressed by national regulators (see Clifford Chance Talking Tech, Italian court confirms that personal data has economic value in Facebook case). The highly anticipated EU Court of Justice decision in this case may pave the way for greater clarity on how the competition and privacy regulators are likely to interact and resolve tensions between the two regulatory spheres going forward. The German NCA's recent report following its market study into non-search online advertising raised the question of whether restrictions on the collection and/or use of data, driven by privacy and data protection concerns, could result in a less diverse and effective system of online advertising and the consequences for diversity of offers and market players, and/or lead to asymmetrical options to the benefit of large providers like Google; such outcomes resulting in negative consequences for competition (See Bunkdeskartellamt: Sector inquiry online advertising / Report for public discussion). The German NCA considered that these risks would have to be weighed against the risks to users' right to informational self-determination, and determined that further analysis is necessary to account for these various aspects when privacy protection concerns would negatively impact competition.

The comments from the Commission in its *Google AdTech* case (see Specific data-related concerns that EU competition law, competition policy, and recent competition law-inspired regulation seek to remedy, *above*) are also significant in this respect, supporting the growing convergence between competition and privacy law and highlighting the need for these to "*work hand in hand to ensure that display advertising markets operate on a level playing field in which all market participants protect user privacy in the same manner*" (see Commission Press Release). In 2020, the Commission took the view in its *Google/Fitbit* decision that the role of competition law is not to protect against and remedy privacy issues (see Case M.9660 Google/Fitbit, *paragraphs 410 to 413, and 452*). Rather, these are better addressed through data protection tools (for example, GDPR). This arguably conservative view of the purpose of merger review and the interests competition law should protect has led to criticism, with commentators arguing that the Commission failed to adequately take account of privacy concerns in *Google/Fitbit*, resulting in the remedies imposed being insufficient to protect consumers' data. Whether the Commission takes similar approach to the role of competition law and the weight given to privacy concerns in the *Google AdTech* case may be a decisive moment for the interplay between these two fields going forward.

From an enforcement standpoint, the interconnection between competition, privacy and data may add an additional layer of complexity once the Data Act proposal becomes applicable, as Article 31 of the Data Act proposal provides that each Member States must designate at least one competent authority as responsible for applying and enforcing the Data Act. The proposal outlines that the national DPAs shall be responsible for the application of the Data Act insofar as the protection of personal data is concerned and Article 33(3) thereof references the GDPR (specifically Article 83(3)(5)) also in relation to penalties, meaning that fines for breaches of the Data Act may result in administrative fines up to EUR20 million or 4% of turnover, whichever is higher. However, the Data Act proposal does not elaborate much further on the potential relevance of breaches of the Data Act for privacy or competition purposes. In fact, while of course the amount of fines referenced to in the Data Act proposal is potentially significant, it remains to be seen whether violations of the Data Act will only be assessed as such, or in relation to their ability to restrict competition or to hinder the exercise of privacy rights, or both.

DPA and NCA case law already includes cases where a potential breach of the GDPR was sanctioned by a NCA because it resulted in a limitation of competition. For example, the Italian NCA imposed a penalty on Facebook, on grounds that Facebook "*was not adequately informing consumers registering on the social network about the collection and use of their personal data for commercial purposes and, more generally, about the remunerative aims underlying the supply of the service, while at the same time emphasising that it is provided free of charge* [resulting in Facebook carrying] *out an unfair commercial practice, inducing users to make a transactional decision they would have not otherwise made*" (see Case IP330-ICA press release). Once the Data Act comes into force, several of its provisions, if breached, could severely hinder competition or privacy rights, thereby raising complex jurisdictional issues among various authorities.

This article was originally published on Thomson Reuter's Practical Law.

## AUTHORS

**Andrea Tuninetti Ferrari**
**Counsel**
**Milan**
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

**Shruti Hiremath**
**Senior Associate**
**London**
T: +44 207006 3075
E: shruti.hiremath@cliffordchance.com

**Manel Santilari**
**Senior Associate**
**Barcelona**
T: +34 93 344 2284
E: manel.santilari@cliffordchance.com

**Antoaneta Shikerova**
**Trainee Lawyer**
**Rome**
T: +39 064229 1264
E: antoaneta.shikerova@cliffordchance.com

**Alice Keunen**
**Trainee Solicitor**
**London**
T: +44 207006 2739
E: alice.keunen@cliffordchance.com

## CONTACTS

**Dessislava Savova**
**Partner**
**Paris**
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

**Nelson Jung**
**Partner**
**London**
T: +44 207006 6675
E: nelson.jung@cliffordchance.com

**Jonathan Kewley**
**Partner**
**London**
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

**Dieter Paemen**
**Partner**
**Brussels**
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com

**Michael Dietrich**
**Partner**
**Düsseldorf**
T: +49 211 4355 5542
E: michael.dietrich@cliffordchance.com

**Thomas Voland**
**Partner**
**Düsseldorf**
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

**Gail Orton**
**Head of EU Public Policy**
**Paris**
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

**Rita Flakoll**
**Senior Associate**
**Knowledge Lawyer**
**London**
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

**Alexander Kennedy**
**Counsel**
**Paris**
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

**Andrei Mikes**
**Senior Associate**
**Amsterdam**
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

**Herbert Swaniker**
**Senior Associate**
**London**
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

**Stavroula Vryna**
**Senior Associate**
**London**
T: +44 207006 4106
E: stavroula.vryna@cliffordchance.com

CLIFFORD

CHANCE



www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ



2303-005281