CLIFFORD

CHANCE

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

PART TWO – DATA ACCESS

DATA ACCESS

This is the second chapter of our paper examining EU Data Act proposal and its interaction with EU competition and privacy regimes. For the full paper please see: The EU Data Act proposal and its interaction with competition, privacy, and other recent EU regulations.

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.

CLIFFORD

CHANCE

www.cliffordchance.com

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

2303-005281