The Consumer Voice in Europe

ACCESS TO CONSUMERS' DATA IN THE DIGITAL ECONOMY

Position Paper

Contact: Agustin Reyna - digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2019-068 – 13/11/2019

Why it matters to consumers

In an increasingly digitalised economy, data is a crucially important component to develop innovative products and services. However, consumers often cannot fully control what happens with the personal data companies gather and process about themselves. Thus, a healthy digital ecosystem requires a consumer-centric approach to data governance that fosters competition, consumer choice and valuable innovation. Determining who has access to data, including consumers' personal information, and under which circumstances and conditions it can be used, are key elements for achieving a healthy and competitive digital economy that delivers benefits to consumers.

Summary

This paper outlines BEUC's position about how to approach personal data access by firms in view of creating a competitive ecosystem for data-driven goods and services. As data is an indispensable input for companies to compete on their merits, it is essential to ensure this indispensability does not result in a race to the bottom undermining the rights of consumers under data protection and consumer protection laws and the consolidation of privacy-intrusive business models.

If companies want consumers to trust their products and services that require access to and process personal information, it is fundamental that consumer interests remain a focus of policies related to data access and control.

BEUC recommends that decision-makers (e.g. when regulating data access regimes) and enforcement authorities (e.g. when designing data access remedies) take into account the following principles for a consumer-friendly data-driven and competitive ecosystem:

- *Intervention in the form of data access should be used only to tackle market failures leading to higher consumer prices, less choice and less innovation.*
- *Data access must foster the development of consumer-centric innovation.*
- *Consumers must be allowed to object to the sharing of their personal data. This right currently does not exist under the General Data Protection Regulation (GDPR) and therefore should be further considered by the legislator as an additional requirement when adopting data access regimes or as a condition for the data sharing if mandated by a competition authority as an interim measure or competition remedy.*
- *Operators handling personal data must be obliged to establish a high-level of data security.*
- *Consumers must be offered technical solutions to help them to control and manage flows of their personal information.*
- *Consumers must have access to redress when these principles are not respected.*
- *Open data initiatives that promote the common interest must be encouraged.*

Introduction: A new economic and social order

Data is part of a new economic and social order. Data impacts how companies innovate. Many firms see data as a crucial input for the development of online services, optimisation of production and the take-up of new technologies such as artificial intelligence[1]. At the same time, data can affect how public bodies design and implement their policies and, ultimately, how consumers are able to enjoy the benefits of digital technologies in a safe and secure manner. The digital revolution has brought and has the potential to bring even more benefits to consumers and society but has also raised new concerns stemming from the collection, aggregation and use of data from consumers. In Europe, this situation also has a fundamental rights dimension since personal data and privacy are protected by the EU Charter of Fundamental Rights.

From a consumer viewpoint, the use of data gives rise to two main concerns. First, it is important to ensure that data collection practices do not lead to concentration of information and of market power, and that consumers are not deprived of innovative services because the companies that hold data do not want to grant access to rivals or downstream or upstream market operators. Second, companies tend to aggregate more data than the consumer would normally expect or want. The data collected could be used to build detailed profiles of consumers and used against their interests, undermining their rights (e.g. price discrimination or manipulation of consumer demand).

Companies have different data 'needs' depending on the services they develop and the sectors of the economy they are active in. However, there is general agreement on the fact that whoever controls access to data has a greater ability to innovate and to bring new products and services onto the market. Holding sufficient data has become a strategic business requirement for developing artificial intelligence and automated decision-making tools, which are and will be increasingly used in all sectors of our economy. Data holders decide ultimately on how to use consumer data. While often creating the perception that consumers control their own data, data holders in practice control the extent to which innovative products are brought to the market by restricting access to consumers' personal data and how it can be used. This leads to market entry barriers and acts as a disincentive to innovate with privacy-enhancing technologies. Thus, these practices can lead to a spiral of inefficiencies in digital markets that harm consumers and disrupt competition.

Moreover, data-driven business models can impact consumers from an economic, political and social perspective. New forms of economic and non-economic harm caused by behavioural manipulation[2] have emerged as a result of data processing, e.g. exclusion when accessing information sources as a result of echo chambers, behavioural discrimination and personalised pricing[3]. This results in consumers feeling disempowered in the face of companies and the way they use their data. For example, a report by UK consumer organisation Which? showed high levels of concern about how firms use individuals' personal information[4]. Similarly, the Norwegian Consumer Council demonstrated how consumers are being forced to continuously share data through the use

[1] J. Crémer, Y-A. de Montjoye and H. Schweitzer, "Competition policy in the digital Era", final report, April 2019.
[2] See: The Behavioural Insights Team, "The behavioural science of online harm and manipulation, and what to do about it", report, April 2019: <https://www.bi.team/wp-content/uploads/2019/04/BIT_The-behavioural-science-of-online-harm-and-manipulation-and-what-to-do-about-it_Single.pdf>.
[3] BEUC note for the OECD on personalised pricing in the digital era, November 2018, <https://one.oecd.org/document/DAF/COMP/WD(2018)129/en/pdf>.
[4] Which?, "Control, Alt, Delete? The future of consumer data", report, June 2018: <https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report>.

of 'dark patterns' and misleading interface design[5]. While these reports raise serious concerns from a data protection and consumer law viewpoint, they also underline the need to decentralise and distribute fairly the benefits generated by consumers' data in the form of consumer-centric innovation.

Decision-makers and enforcers can play an important role in this regard, not only by giving consumers strong rights, empowering and protecting them (e.g. data protection and consumer rights), but also by steering markets to ensure that they deliver benefits for consumers and by preventing anti-competitive behaviour.

While there is already a very relevant policy debate about how to deal with data from a market perspective, this paper focuses on the access and use of data from a consumer perspective.

Wanted: a European consumer-oriented data access and control policy

Europe is a front runner in the field of consumer protection, data protection and privacy. Consumers in Europe enjoy the highest levels of data protection in the world[6] and Europe's consumer laws have been upgraded to better protect consumers in the digital economy[7]. However, there are still gaps about how to deal with data from an economic and societal perspective. Additional measures are needed to make sure that consumers' data is used in ways that leads to valuable innovation.

It is important to highlight that a distinction between personal and non-personal data is very often not possible. For example, it is often difficult to distinguish between personal and non-personal data generated by consumer devices (e.g. from connected vehicles, smart appliances and smart meters): even if data have been anonymised, consumers can be re-identified. Thus, we consider that these data are personal data under the terms of the General Data Protection Regulation (GDPR) as they are likely to relate to the individual owner or user of the product. Where data sets combine both personal and non-personal data, the European Commission in its guidance on the implementation of the Regulation on a framework for the free flow of non-personal data in the European Union[8] highlighted that "*if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset*." This principle should also be applied in any future EU data access regimes in situations of mixed data sets: it means that in most cases involving consumer products and services, the GDPR will be fully applicable to all data generated by the devices or service interactions.

A European consumer-oriented data access and control policy is necessary to define the framework and conditions for accessing and using consumers' data: who should be entitled

[5] Norwegian Consumer Council, "Deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy", report, June 2018: <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

[6] See for example the General Data Protection Regulation and the ePrivacy Directive, currently under revision.

[7] See for example the new EU rules on digital content and digital services and on sales of goods: Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services *OJ L 136, 22.5.2019, p. 1–27 and* Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC *OJ L 136, 22.5.2019, p. 28–50.*

[8] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM/2019/250 final.

to have access, for what purposes and how can consumers remain in control and grant access to their data according to their needs?

There is general agreement that data concentration in the hands of a few market players, and barriers to access the data legally held by such players, are problematic from an economic and societal viewpoint[9]. However, there is no clear regulatory vision about how to deal with this issue. This is because the regulatory architecture of the data economy is fragmented and incomplete. The GDPR provides the general legal framework that implements the fundamental right to data protection and regulates the processing of personal data. However, the GDPR does not apply to non-personal data (often refer to as industrial data) and does not address data access issues beyond the compliance of personal data processing practices with the principles, rights and obligations established in the Regulation. Another problem is that the recently adopted Regulation on the free flow of non-personal data fails to address data access as a market failure since it relies on industry-led self-regulation for the portability of non-personal data[10]. Thus, there is a need to further explore how best to address the role of data in the digital economy and society both from a market and a consumer perspective.

A focus on access and control of data by data holders and third parties represents the best way forward to stimulate competition whilst ensuring consumers remain in control of their data. This 'access and control' approach has very practical consequences:

- First, without having to assign ownership of data to any specific person or entity, it allows the development of different data access regimes that, in compliance with the GDPR and the e-Privacy Directive, would enable consumers greater control over their data and would allow different parties to access data necessary to provide innovative services. While it is important to provide the necessary incentives for markets to be competitive, we must guarantee that consumers are in control of their personal data.

- Second, for everything that involves consumers' and citizens' data, data access regimes must always operate in compliance with the rights, obligations and principles established in the GDPR[11]. Except in case of a legal obligation on a company to share data, it is the consumer who ultimately should give permission for the collection and use of personal data within the protection granted by the mandatory nature of the GDPR. Further to this, additional protection complementing the GDPR in sector specific data access regimes (e.g. on further conditions or limits on the use of certain categories of data, for example in the health sector, or further practical requirements to obtain consent) can also be necessary and should be adopted accordingly.

- Third, data access regimes can target market failures more precisely in different sectors. For example, an access regime related to open banking would have different requirements compared to the data access regime in the new Energy Directive concerning the data held by the Distribution Network Operators (DSO)[12].

---

[9] J. Drexl, "Data access and control in the era of connected devices", study for BEUC, <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf>.

[10] Article 6 of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303, 28.11.2018, p. 59–68.*

[11] See in this regard the research carried out by J. Kühling for our German member, vzbv, "Rechte an Daten", <https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf>.

[12] The revised Electricity Directive which sets rules on the exchange of data among energy suppliers and aggregators as well as on non-discriminatory access to data. Broadly speaking, Member States should put in place rules under which data can be accessed under non-discriminatory conditions and ensure cybersecurity and

Similarly, any eventual data access and interoperability obligation to open-up online messaging services like WhatsApp or Telegram[13] would require technical specifications that would differ from those required in legislation related to accessing data by independent repair centres for the provision of after-sales services for vehicles[14]. But what all these regimes have in common are the requirement that consumers remain in control of their data when firms access and use consumers' data.

The current European framework applicable to data access and control

European laws provide substantial rules that address data-related issues from different perspectives (e.g. ensuring competition, protecting consumers' rights and individuals' personal data, protection of trade secrets[15] or intellectual property). These horizontal instruments are coupled with sectoral legislation which address specific situations regarding data access and control (e.g. the Open Data Directive[16], Payment Services Directive 2[17]and the Type Approval Regulation[18]).

If we look at data as an input for the development of goods and services, the main basis for addressing lock-in effects is primarily found in **EU competition law**. However, the scope for intervention in this area can be limited. Within the EU competition law framework, a refusal to grant access to data could be seen as a case of refusal to deal, which is sub-category of an abuse of dominance under Article 102 TFEU. However, in practice the application and enforcement of this rule creates considerable challenges. First, an abuse can only be proven if the data holder holds a dominant market position. Secondly, the 'refusal to deal' has to constitute an abuse[19]. Under EU competition law, such an abuse requires a refusal to supply an indispensable input, thereby preventing the petitioner from competing in a downstream market. However, it is not clear whether data collected by companies can constitute an indispensable input under EU Court of Justice case law[20].

The second horizontal instrument that plays a role in this area is the **General Data Protection Regulation** (GDPR). This instrument contains some pro-competition provisions like the portability right (Article 20), but it falls short of addressing lock-in

data protection as well as the impartiality of the entities which process data. Member States or competent authorities should specify the rules on the access to data of the final customer by eligible parties.

[13] Electronic Frontier Foundation, "Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Remedies": <https://www.eff.org/es/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine>.

[14] Article 65 of the Type Approval Regulation provides that *"manufacturers shall provide to independent operators unrestricted, standardized and non-discriminatory access to vehicle OBD information, diagnostic and other equipment, tools including the complete references, and available downloads, of the applicable software and vehicle repair and maintenance information. Information shall be presented in an easily accessible manner in the form of machine readable and electronically processable datasets. Independent operators shall have access to the remote diagnosis services used by manufacturers and authorised dealers and repairers."*

[15] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157, 15.6.2016, p. 1–18.*

[16] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172, 26.6.2019, p. 56–83.*

[17] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, *OJ L 337, 23.12.2015, p. 35–127.*

[18] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, *OJ L 151, 14.6.2018, p. 1–218.*

[19] The leading case in this regard is the *Bronner* case, dealing with access to a nation-wide home delivery system for daily newspapers.

[20] J. Crémer, Y-A. de Montjoye and H. Schweitzer, "Competition policy in the digital Era", final report, April 2019, p. 101-105.

effects. Article 20 of the GDPR therefore provides for a general right to data portability as regards personal data, which is not just a right to strengthen the data subject's autonomy, but has been conceived as a tool to *'support the free flow of personal data in the EU and foster competition between controllers'*[21]. However, this right has several limitations. First, it applies only to personal data. Secondly, the portability right applies to data "provided" by the data subject. This should include all raw data generated by the consumer through the use of the service, and also data inferred by the data controller. However, the GDPR is not clear about this issue. Finally, the portability right laid down in the GDPR does not impose any interoperability obligations enabling companies entering the market to interact with the data holders' service. The **Free Flow of Data Regulation** (Article 6) also deals with the portability of non-personal data between firms but it does not tackle market failures stemming from the incumbent's refusal to grant access to data since it relies on self-regulation without assigning any data access right to third-parties . And, the recently revised **Public Sector Information Directive**[22] provides for a legal framework for the access, user and re-use of public data, including publicly-funded research data, that can help to optimise public services but also allow companies, especially start-ups, to develop innovative products and services.

This insufficient legal framework, as well as the difficulty of enforcing competition law in each case, strongly argues in favour of taking additional legislative action outside the realm of competition and data protection laws. Progress has been made in sectoral legislation. Mandatory data access and interoperability exists in **sector-specific EU laws** in the field of financial services, after-sales services for vehicles and energy grid data: namely the Payment Services Directive (PSD2), the Type Approval Regulation and the revised Electricity Directive. These instruments impose obligations on the data holders or incumbents to enable access to data, for example in the case of open banking, through an application programming interface (API), so that other operators are able to provide services to consumers. Although the nature of the data concerned is different, due to the particularities of the markets concerned, the obligations under these instruments all seek to address market failures. These pro-competition measures are designed in the light of that objective, something that it is not necessarily the case with other EU laws, which aim to protect other issues (e.g. data protection or intellectual property). But these examples of pro-competition legislation often fail to deal specifically with the role of consumers in such access regimes, in particular concerning consumer permission to access his or her personal data as it is discussed further below.

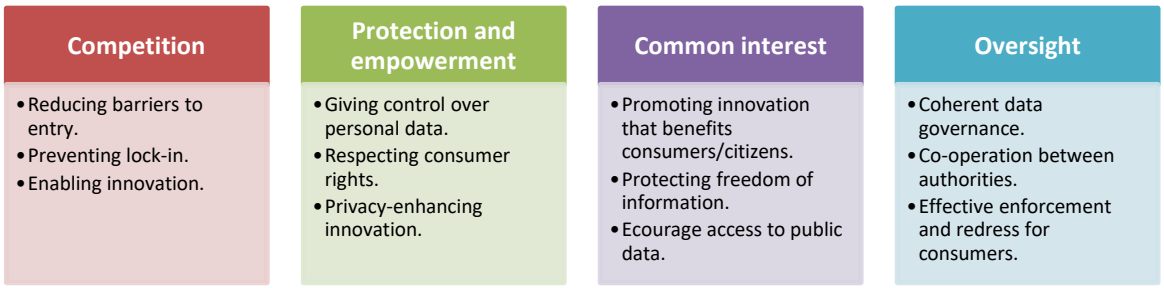
A consumer-oriented vision for a European data access and control policy

A European data policy should provide the foundations for the access and use of data across different sectors in the European Union. It should establish who should be entitled to access data held by another party, under what conditions and for what purposes. Since most of this data is generated by consumers when they use devices and digital services, and therefore can be considered as personal data, it is essential that access regimes guarantee the highest levels of consumer protection and consumer empowerment.

Thus, BEUC considers that a consumer-centric European data policy should be built around four pillars to ensure that data is used for the benefit of consumers, namely promotion of a competitive data economy, protection of consumers' rights and consumer empowerment, promotion of the common interest and strong regulatory oversight.

[21] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (13 December 2016; revised 5 April 2017).

[22] European Commission, 'Digital Single Market: EU negotiators agree on new rules for sharing of public sector data', Press Release: <http://europa.eu/rapid/press-release_IP-19-525_en.htm>.



1. Competitive data economy

Access to data is important to reduce barriers to entry and address lock-in effects. Market failures happen when market players have an interest to access data to develop services and products, while the data holders are not obliged to provide them access to their data but are able to control innovation and capture the demand entirely. The same applies when companies with significant market share refuse to interoperate or allow other firms to interact with consumers e.g. by accessing the users' interface (even when users give consent). This has significant consequences because, as indicated above, having access to data is a pre-condition to compete. Thus, pro-competitive data access regimes complementing competition law enforcement should seek to decentralise the data held by data holders whilst maintaining incentives to innovate for the benefit of consumers.

2. Protection of consumers' rights and consumer empowerment

Guaranteeing the conditions for innovation and competition to thrive should go hand-in-hand with the protection of consumers' rights. This implies that any data access regime, and the data practices derived from such a regime, should ensure that consumer rights, and in particular data protection rights, are upheld by both the data holders and by those seeking to gain access to data necessary to innovate. Under such a regime, consumers could promote innovation if they retained control over their data. Consumers should be in a position to decide who gains access to their data and under what conditions. A pre-condition for markets to be competitive is to empower consumers to make informed decisions about how firms use their data. Currently, consumers do not know or understand how firms handle their personal data when providing a service. In such an environment, consumers are highly vulnerable to be manipulated by businesses, which may lead to concrete economic and social harms (e.g. discrimination). This situation calls for the adoption of special consumer protection, for example in the context of automated decision-making technologies[23].

3. Promotion of the common interest

Access to data can also enable governments, agencies and non-governmental organisations like consumer groups to fulfil their mandates more efficiently and develop services in the benefit of the common interest. Such data can be held by both private and public entities. For data held by public entities the recently revised Public Sector Information Directive[24] provides the legal basis for making data from publicly-funded services widely and freely available. This is a step into the right direction, which will enable a wide range of actors to access data necessary to develop new services of common

[23] BEUC, "Automated-decision marking and Artificial Intelligence – A consumer perspective: <https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf>.

[24] European Commission, 'Digital Single Market: EU negotiators agree on new rules for sharing of public sector data', Press Release: <http://europa.eu/rapid/press-release_IP-19-525_en.htm>.

interest and value. Enabling access to data held by public entities is in line with the spirit of the right to freedom of information under the EU Charter of Fundamental Rights.

4. Strong regulatory oversight

The EU currently lacks a co-ordinated governance structure to deal with data-related issues. Different sector authorities may simultaneously or consecutively intervene depending on the material and territorial scope of application of the laws and regulations they are competent to enforce. Progress has been made at national level with cross-agency initiatives in France, Germany and Norway. However, there is a need to streamline enforcement also at EU level where certain illegal and unfair business practices by data holders can have cross-border implications. While the new "consistency mechanism" of the General Data Protection Regulation (Article 63) provides an innovate instrument to ensure that EU wide infringements can lead to one European wide and coherent response by all national data protection authorities, a corresponding measure to ensure that consumers are compensated if they suffer harm because of such an infringement does not exist yet across the EU. Further to this, it is essential that authorities have enough resources and powers to increase their analytical capability to be able to understand these complex markets.

In addition, the creation of specific bodies supporting the work of competition, consumer and data protection authorities, which can be entrusted with the oversight of data markets and the use of data by market operators could be envisaged. Similar initiatives have been suggested at national level: For example, the UK "Furman" report recommends the creation of a digital markets unit within the competition authority dealing with data mobility systems and open data[25].

Finally, building stronger synergies between public and private enforcement can contribute to a culture of compliance and ensure that consumers obtain redress when their rights are violated. For example, several of our members have undertaken actions against companies for violating consumer or data protection laws. Test-Achats/Test-Aankoop (Belgium), Altroconsumo (Italy), DECO (Portugal) and OCU (Spain) are bringing together over 150,000 consumers in representative group actions against Facebook for the harm suffered due to the violation of their consumer and data protection rights in the Cambridge Analytica case and our French member UFC-Que Choisir launched a collective action against Google for infringing multiple laws[26].

Models of data access from a consumer perspective

Data access can take place in different ways. There are in our view two models of personal data sharing that require special attention. The first model relates to data access mandated by the legislation or an enforcement authority (e.g. competition agency) in which a data holder is required to provide access to the data of its customers to another market operator (e.g. rival or an upstream or downstream market player). This model promotes the development of competitive markets. In the second model, it is the consumer who initiates the process by requiring a market operator to provide a service that needs to access the customers' data from a data holder in order to provide the service. This model promotes the individual interest of consumers, who take an active role by initiating the data sharing.

[25] Report of the Digital Competition Expert Panel, "Unlocking digital competition", March 2019, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf>.

[26] UFC-Que Choisir, Vie privée. Action de groupe contre Google, June 2019: <https://www.quechoisir.org/action-ufc-que-choisir-vie-privee-donnees-personnelles-action-de-groupe-contre-google-n68403/>.

Below we assess how these models operate from a consumer perspective. Such models can coexist and should be considered depending on the market failure that needs to be addressed.

1. Model A: mandating data access

Under this scenario, by law or by a decision of an authority like a competition agency, a data holder must allow another party to access its customers' data. This was the case, for example, in the interim measure ordered by the French competition authority in the GDF Suez merger[27]. In this case, a direct rival of GDF Suez (Direct Energie) requested access to its customers' data base (including meter number, annual consumption, name and surname of the clients, billing address and fixed telephone number) under gas regulated tariffs to allow gas suppliers to inform customers of alternative offers and therefore compete more efficiently with GDF Suez. Upon consultation with the French data protection authority, the competition agency allowed the disclosure of data provided that consumers were allowed to opt-out from the GDF Suez customer list[28].

It is important to highlight that these types of cases are the exception and imply an important and delicate trade-off between guaranteeing more competitive markets and the protection of the individual's personal data.

From a BEUC perspective, this balancing exercise must not be misused to allow a free flow of personal data without a proportionate and well-founded pro-competition justification since the protection of consumer's personal data is a fundamental right and as such can only be subject to limitations in specific circumstances. Further to this, agencies and regulators should not take a liberal approach to the use of personal data and assume that any data can be used to promote competitive markets. On the contrary, only defined categories of data that are indispensable to attain specific objectives and purposes should be subject to mandated access. Thus, data access regimes or decisions by authorities need to follow clear criteria about the conditions for data sharing so that consumers remain in control:

- Firstly, the conditions for data sharing need to be defined by a legislative instrument, e.g. in a sector specific data access regime, complementing – but not weakening or contradicting – the GDPR. In this regard, we encourage the European Commission when proposing new legislation related to data access or when considering data access as a competition remedy to ask for an opinion from the European Data Protection Supervisor.

- Second, consumers should be given the option to object to data sharing between companies when the sharing has been mandated by law. Such a right to object does not exist under the GDPR since in this situation the data sharing would be considered a legal obligation and constitute a legal basis for processing under Article 6(1)(c) of the GDPR to which the right to object of Article 21 does not apply. However, a right to object data sharing as part of data access regimes would specify the conditions for the compliance with the legal obligation by companies required to grant access to the consumers data.

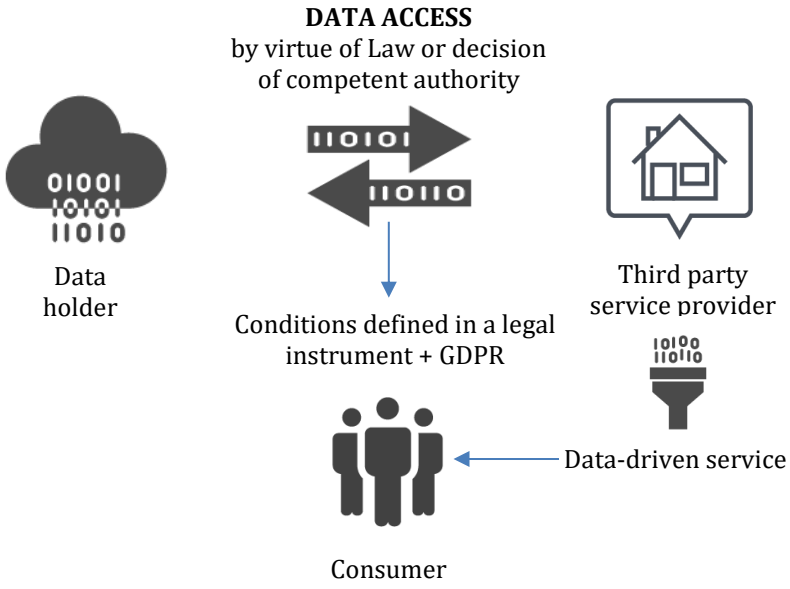
[27] Décision n° 14-MC-02 du 9 septembre 2014relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité:
<http://www.autoritedelaconcurrence.fr/pdf/avis/14mc02.pdf>.

[28] The following disclaimer was introduced: *'Si vous ne souhaitez pas que vos données soient transmises à des fins de prospection commerciale aux fournisseurs ayant fait une demande d'accès à la base de données clients de GDF SUEZ, veuillez renvoyer le formulaire en cochant la case ci-contre. À défaut d'opposition de votre part dans les 30 prochains jours, vos données seront automatiquement rendues accessibles à ces fournisseurs'.*

- Third, When data access is mandated by an competition authority, for example as a result of an interim measure or a remedy, the authority upon consultation with the national data protection authority (or in the case of the European Commission upon consultation with the European Data Protection Board), should require as part of the measure that consumers are allowed to opt-out from the data sharing.

- Fourth, decisions to mandate disclosure and access to data should not be adopted without agreement by relevant data protection authorities and must include all necessary safeguards to protect consumers' data protection and privacy rights. Monitoring of compliance with the disclosure decision is essential to ensure that consumers' data is safeguarded and that the firm concerned will not use the data in a way incompatible with the decision or with the GDPR.

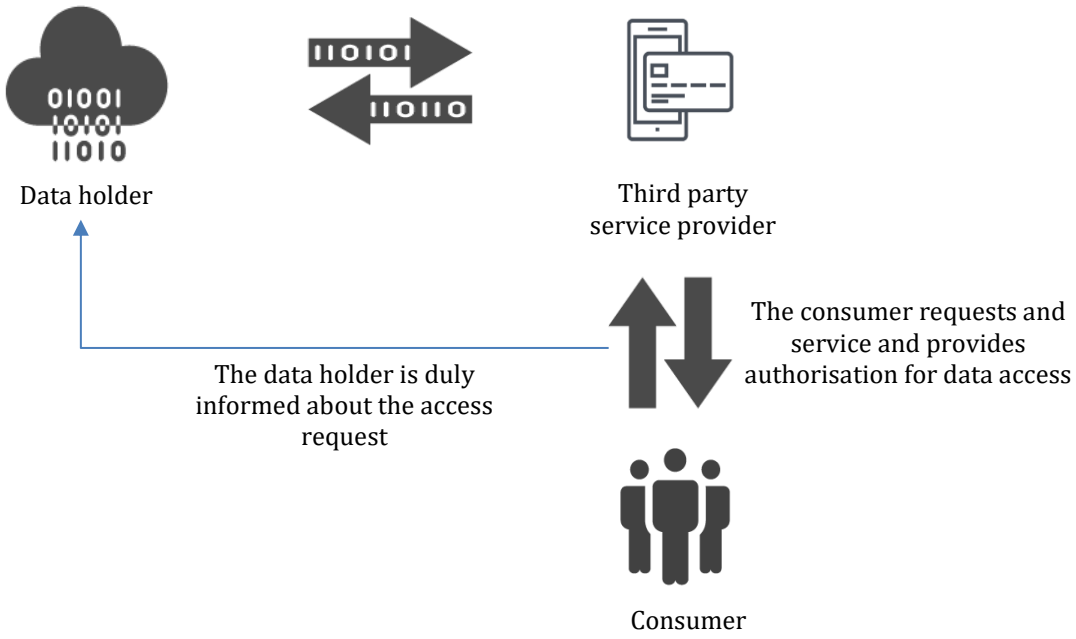
- Finally, there should be technical means in place to allow the consumer to control and manage data flows between firms in a certain market (e.g. through a user dashboard).



2. Model B: data access necessary to provide a service

In the second model, the consumer requests a third party to provide a service that requires the third party to access the consumer's personal data held by the data holder. This is the case for example in open banking: the consumer requests a Third-Party Provider (TTP) to provide a service and the TTP should get secure access to the consumer data from the consumer's bank through an application programming interface (API) so as to be able to provide a payment service. This model can also apply to any service provider, including non-governmental organisations like consumer groups[29], that need to access consumers' data to provide a service.

[29] For example, the Spanish consumer organisation OCU developed in 2014 an application called Mooverang that helped consumers to have a better overview over their finances, which required the access of financial data: <https://www.ocu.org/dinero/cuenta-bancaria/noticias/mooverang>.



In this scenario, it is important to ensure that the data holder is informed unequivocally of the consumer's consent before they grant access to the consumer's data to a third party. This is currently not the case under PSD2 in which the consent is only given to the third-party payment provider and not to the customer's bank[30]. Under PSD2 the bank cannot even verify the consent given to the third-party provider, which is problematic. Further safeguards are therefore needed. Any future legislation on data access for the provision of consumer services needs to take into account how the different parties involved in the transfer of data will be informed of the consumer's permissions and needs to include more protective provisions than the existing access regime. It is also very important to ensure that only the data that is necessary for the provision of the third-party service is accessed. In a nutshell, this model should not be used to circumvent personal data protection rules. In this regard, BEUC has already made a set of recommendations when following this model in the PSD2 [31], including:

- Explicit consent required under sector-specific legislation should mirror the requirements of explicit consent under the GDPR, regardless of what the legal basis for processing is under the GDPR.

- Strong data minimisation and purpose limitation must be ensured. Consumers should be able to control which data they give access to and services should not access more data than they need to provide the service requested by the consumer. Further processing of account data for compatible purposes should be strictly limited.

- Access to data that might reveal information considered sensitive under Article 9 GDPR should be separated from access to other data.

- Strong co-operation between sectoral authorities and national data protection authorities is crucial for effective and meaningful protection of consumers.

[30] See BEUC's recommendations to the EDPB on the interplay between the GDPR and PSD2: <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf>.
[31] *Ibid.*

Case study: access to in-vehicle data

The automotive sector gives rise to concerns regarding access to in-vehicle data by third parties. The data generated by vehicles is already and will increasingly be key for the after-market services and for a wide range of new mobility services which might arise from greater connectivity. Therefore, it is essential to ensure that access to in-vehicle data is fair to all service providers and enables true competition while ensuring full respect of data protection laws. This debate is very similar to the past debate around availability of spare parts for after-sales markets but with a new dimension: data will be the basis for every service, every operation to be carried out by a wide range of service providers, not only repair centres. Thus, the competition concerns stemming from refusing access to in-vehicle data are even greater because they will affect many mobility-related markets.

There are growing concerns about the efforts of the car industry (spearheaded by their trade body ACEA) to control access to data through the so-called "extended server"[32]. Such criticisms come from a wide range of players including independent repairers, car rental companies, car clubs, insurance companies and new mobility service providers. These concerns on the risk of disruption to competition are substantiated by different studies. First, the study of the Joint Research Centre[33] concluded that the extended vehicle model proposed by the car industry "ensures their data access monopoly and enables them to maximize revenue from data and data-driven aftersales services. It reduces welfare for drivers and aftersales service providers"[34]. Second, a study commissioned by DG MOVE (known as the TRL report)[35], also emphasised that the extended vehicle/neutral server model bears significant risks in terms of fair competition. More recently, FIA (Fédération internationale de l'automobile) also published a report showing that the proposed model could significantly increase costs for independent market players and prices for consumers[36].

Car manufacturers often claim the extended vehicle model is much safer in terms of cybersecurity, which is of course a very valid argument especially in the case of self-driving cars. But there are no studies or evidence that the extended-vehicle model would ensure better cybersecurity.

Furthermore, a model in which service providers have one single entry point to access in-vehicle data will allow car manufacturers to always be in a better position to provide services or even to completely exclude other service providers through foreclosure of rivals and entry barriers. Another problematic issue is that we cannot allow outsourcing to a third party the decision of who can access the consumer's car data: that is a decision for the consumer herself and any technical measure needs to be based on this principle. There are no economic incentives for car manufacturers to allow third parties to access data that will be used to compete against them at service level. That is exactly why the legislator had to

[32] ACEA, "Access to data by third party services", position paper, December 2016: <https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf>.
[33] Joint Research Centre, "Access to digital car data and competition in aftersales services", Digital Economy Working Paper 2018-06, <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc112634.pdf>.
[34] *Ibid* p. 4.
[35] TRL "Access to In-vehicle Data and Resources", Final report, May 2017: <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf>.
[36] FIA, The Automotive Digital Transformation and the Economic Impacts of Existing Data Access Models", Report, March 2019: <https://www.fiaregion1.com/wp-content/uploads/2019/03/The-Automotive-Digital-Transformation_Full-study.pdf>.

intervene first regarding spare parts and most recently in the Type Approval Regulation as regards to information related to repairability[37].

Given this evidence and the growing concerns expressed by a number of players, we have called upon the European Commission to scrutinise ACEA's extended vehicle model from a EU competition law compliance perspective and to consider launching a sector inquiry into automobile data to better understand the market dynamics surrounding the use of in-vehicle data for after-sale services and related mobility services[38]. This investigation should not prevent the European Commission from considering specific-sector legislation on in-vehicle data access, complementing the requirements of the Type Approval Regulation.

BEUC recommendations for consumer-oriented data access policies

Policymakers must ensure that consumers are at the centre of any legal instruments or measures related to data access on the basis of the following checklist. Each of these recommendations seek to stimulate competitive digital markets while guaranteeing a high-level of consumer protection:

1. Address market failures

Decision-makers and competition law enforcers need to design their policies and measures to ensure they tackle specific market failures stemming from lock-in effects and refusal to grant access to data so that market entrants can provide innovative products to consumers and compete on their merits. These measures should be proportionate and competition-oriented while maintaining the incentives for de facto data holders to innovate in a way that benefits consumers. Such an approach will benefit not only competitive markets but can also contribute to a more sustainable supply chain. For example, such policies and measures can enable after-sales service providers to access the data necessary to provide convenient and affordable repair and maintenance services to consumers, which can contribute to extending the lifespan of products in accordance with the objectives of the circular economy.

2. Stimulate innovation

Intervention in the form of data access regimes or remedies needs to be oriented to the development of innovative products and services that improve market conditions for consumers by encouraging the development of new and higher quality products. It is therefore important for decision-makers (legislators or authorities) to assess whether the data that is going to made available will lead to products and services that will contribute to the well-being of consumers. While it might be difficult to define what is valuable innovation (any company can argue that they contribute to economic and societal progress and generate efficiencies for consumers), the EU institutions have a responsibility to steer innovation to maximise consumer welfare.

3. Put the consumer at the centre in data sharing

Data sharing must respect the safeguards set out by the GDPR. This is the only way to ensure that consumers' personal are protected. Further to this, BEUC considers

[37] Article 61 of Regulation (EU) 2018/858 of 30 May 2018.
[38] Letter to Commissioners Vestager and Bulc of 11 October 2019, <https://www.beuc.eu/publications/beuc-x-2019-058_letter_to_commissioner_vestager.pdf>

that where the legislation mandates data access, or such access is a result of a decision by a public authority that a data processor is required to share data with third parties (legal obligation), consumers should have the possibility to object to the sharing of their data.

4. Ensure a high-level of data security

A pre-condition for the sharing of consumers' data is that this takes place in conformity with the necessary level of data security. Article 32 of the GDPR (security of processing) imposes the obligation on processors to respect security requirements. However, this provision applies only in relation to personal data and therefore not all data sets involved in the sharing would be covered by this obligation. In this regard, decision-makers should require that the companies involved demonstrate to the competent authorities that the risks surrounding the sharing, irrespective of the nature of the data concerned, are minimised before the data sharing takes place.

5. Adopt technical solutions to help consumers control and manage flows of personal information

When, in certain markets, consumer data is transferred between firms e.g. for the provision of services, consumers should be able to control these flows through easy mechanisms like user dashboards that can be developed by regulatory agencies in co-operation with industry, academia, the technical community and consumer organisations. The European Data Protection Supervisor, in its opinion on Personal Information Management Systems (PIMS)[39], highlighted the important role of these technological solutions "to allow third parties to use personal data, for specific purposes, and specific periods of time, subject to terms and conditions identified by the individuals themselves, and all other safeguards provided by applicable data protection law". However, PIMS should not be seen as a means to replace consumer protection measures and to force consumers to pro-actively manage their personal data flows. Consumers should benefit from the protection measures outlined above and PIMS should be seen as an additional facilitator.

6. Make redress available to consumers

Consumers must be able to rely on effective redress mechanisms and obtain compensation in case of financial or non-financial detriment stemming from the sharing of data with third parties, in particular in the event of data breaches and misuse of their data. The GDPR provides for specific redress rights against infringement of consumers' data protection rights. It is necessary to ensure that the parties with whom the consumers' data is shared fall under the liability regime of the GDPR. Furthermore, public and private enforcement should work in tandem in order to deter behaviour regarding data handling that would be incompatible with the GDPR while at the same some allowing consumers to seek redress when their rights are breached. Consumers must also benefit from a collective redress tool for infringement of their data protection rights and their rights under the e-privacy Directive. The pending proposal for a Directive on representative actions should ensure that consumer organisations can represent consumers in such circumstances.

7. Reduce the risks of data concentration and excessive data collection

[39] European Data Protection Supervisor opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

Data sharing implies that a wider number of firms can potentially gain access to consumers' personal information. In order to prevent unintended consequences associated with the amount of data collected, it is essential to ensure rigorous compliance with the principles of the GDPR, in particular purpose limitation, data minimisation and privacy by design and default. Thus, when the data sharing is imposed by an authority, it is essential to ensure that the data shared is necessary and indispensable for the provision of the services in question to consumers, that companies do not gain access to data that they do not need for the provision of the services concerned and that they do not use or share such data for other purposes.

8. Promote the common interest through open data initiatives

Data access policies are just as important for the public sector and the civil society as for the private sector. Decision makers should therefore prioritise open data initiatives in which different governmental and non-governmental actors can access and use such data for the purpose of developing common interest services. Examples of this exist in specific sectors, like telecoms, where the Regulation establishing the Body of European Regulators for Electronic Communications (BEREC) foresees the "modernisation, coordination and standardisation of the collection of data by [National Regulatory Authorities] … in an open, reusable and machine-readable format"[40]. In addition, BEREC started a discussion for the development of an Open Data Platform, and in that context the national telecoms regulators agreed, as a first step, to develop their own Open Data Policy[41]. Open data initiatives have the potential not only to allow and encourage innovation from new market entrants that cannot afford to engage with large companies to gain access to the necessary data or relevant IP but also to enable mission-oriented entities like consumer groups to develop solutions and services that can rely on open source and open data technologies (e.g. applications to help consumers better manage their finances or compare quality of internet services).

END

[40] Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office) *OJ L 321, 17.12.2018, p. 1–35*

[41] BEREC, Report on Open Data policy, October 2018: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8254-berec-report-on-open-data-policy

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).