

Unclassified

English - Or. English

5 June 2020

**DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE**

Consumer data rights and competition – Note by BEUC

12 June 2020

This document reproduces a written contribution from BEUC submitted for Item 3 of the 133rd OECD Competition Committee meeting on 10-16 June 2020.

More documents related to this discussion can be found at
<http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm>

Please contact Ms Anna BARKER if you have questions about this document.
[Email: Anna.BARKER@oecd.org]

JT03462641

BEUC

1. Introduction

1. BEUC welcomes the opportunity to contribute on the Roundtable on “Consumer Data Rights: Impacts on Competition”.

2. 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 intelligence¹. 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.

3. 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).

4. 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 understanding 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, in practice they rather use the opportunity to 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.

5. 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 manipulation² have emerged as a result of data processing, e.g. exclusion when accessing information sources as a result of echo chambers, behavioural

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>.

discrimination and personalised pricing³. 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 information⁴. Similarly, the Norwegian Consumer Council demonstrated how consumers are being forced to continuously share data through the use of 'dark patterns' and misleading interface design⁵. 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.

6. 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.

2. A European consumer-oriented data access and control policy

7. 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 Union⁶ 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.

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

9. 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

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](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>>.

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 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.

an economic and societal viewpoint⁷. However, it is often not clear 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 may fail to address data access as a market failure since it relies on industry-led self-regulation for the portability of non-personal data⁸. 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.

10. 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. 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)⁹. Similarly, any eventual data access and interoperability obligation to open-up

⁷ J. Drexler, “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>.

⁸ 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, *OJL 303*, 28.11.2018, p. 59–68.

⁹ 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 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.

online messaging services like WhatsApp or Telegram¹⁰ 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 vehicles¹¹. All these regimes have a common requirement that consumers remain in control of their data when firms access and use consumers' data.

3. What role for consumer data rights?

11. 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 secrets¹² 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 Directive¹³, Payment Services Directive 2¹⁴ and the Type Approval Regulation¹⁵).

12. 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 abuse¹⁶. Under EU competition law, such an abuse requires a refusal to supply an indispensable input, thereby preventing the petitioner from

¹⁰ 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>>.

¹¹ 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.*"

¹² 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*.

¹³ 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*.

¹⁴ 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*.

¹⁵ 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*.

¹⁶ The leading case in this regard is the *Bronner* case, dealing with access to a nation-wide home delivery system for daily newspapers.

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 law¹⁷.

13. 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 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*'¹⁸. However, this right has several limitations. First, portability only applies to personal data and therefore excludes other data that could be useful to allow portability between services. Secondly, it applies to data 'provided' by the data subject. This should include not only all raw data generated by the consumer through the use of a service, and also data inferred and derived by the data controller. However, according to the European Data Protection Board (EDPB), the portability right under the GDPR seems not to cover data derived or inferred by the data controller. For example, while behavioural data generated through observation of the data subject is deemed as 'provided' by the data subject, this category does not include data generated through analysis of such behaviour¹⁹. From a competition perspective, the portability right of the GDPR does not entail specific interoperability obligations enabling new entrants to interact with the data holder's service²⁰. That is why BEUC welcomes that the Commission plans in the context of its Data Strategy of February 2020 to adopt measures to enhance the portability right under Article 20 of the GDPR in its upcoming Data Act.

14. 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**²¹ 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.

15. This insufficient legal framework, as well as the difficulty of enforcing competition law in each case, strongly argue 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:

¹⁷ J. Crémer, Y-A. de Montjoye and H. Schweitzer, "Competition policy in the digital Era", final report, April 2019, p. 101-105.

¹⁸ Article 29 Data Protection Working Party, Guidelines on the Right to data portability (13 December 2016; revised 5 April 2017)

¹⁹ EDPB Guidelines on the right to "data portability, Ref.: https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_en, (accessed on 31/05/2020), page 10.

²⁰ The EDPB noted however that "data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject's request (Article 12(4))." This does not mean that the services shall become interoperable for which separate technical measures are needed.

²¹ 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>

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 below.

4. Models of data access from a consumer perspective

16. Data access can take place in different ways. There are however 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 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. 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.

4.1. Model A: mandating data access

17. 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 merger²². 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 list²³.

²² Décision n° 14-MC-02 du 9 septembre 2014 relative 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>>

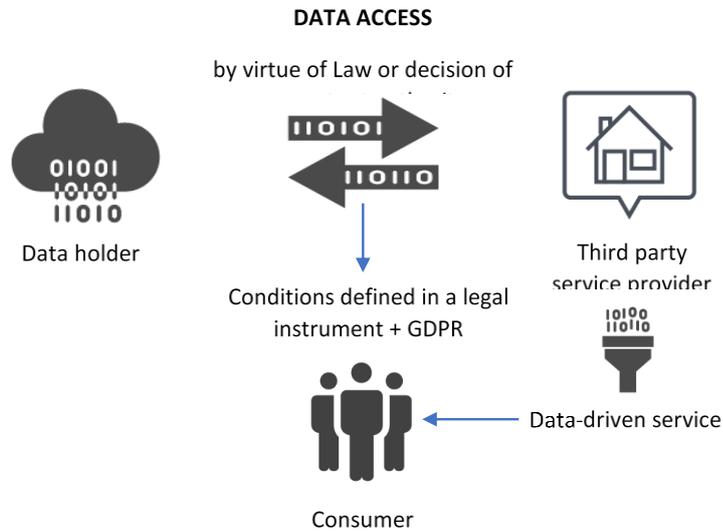
²³ The following disclaimer was introduced: *'Si vous ne souhaitez pas que vos données soient transmises à des fins de prospection commerciale aux fournisseurs ayant fait une demande d'accès à la base de données clients de GDF SUEZ, veuillez renvoyer le formulaire en cochant la case ci-contre. À défaut d'opposition de votre part dans les 30 prochains jours, vos données seront automatiquement rendues accessibles à ces fournisseurs'*.

18. 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.

19. 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, it 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 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.
- 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).

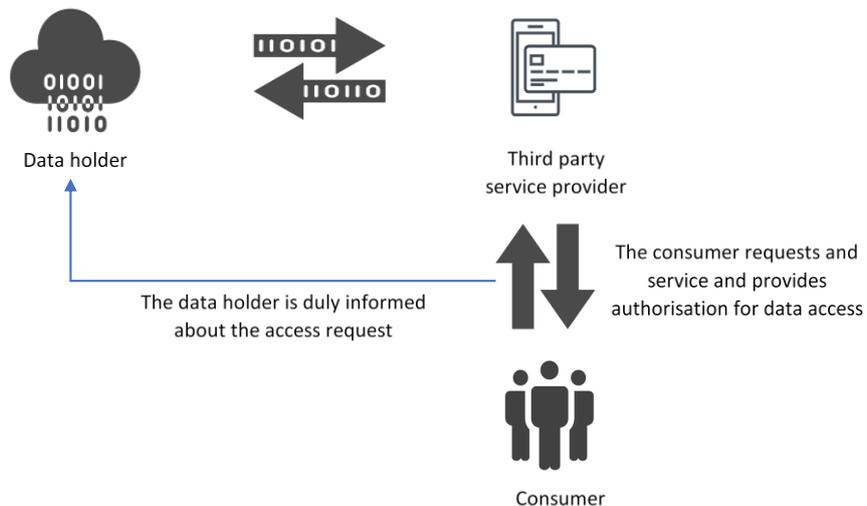
Figure 1.



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

20. 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 groups²⁴, that need to access consumers' data to provide a service.

Figure 2.



²⁴ 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>>.

21. 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 bank²⁵. 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 PSD2²⁶, 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.

5. BEUC recommendations for consumer-oriented data access policies

22. Policymakers must ensure that consumers are at the center 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:

- 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

²⁵ 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>.

²⁶ *Ibid.*

consumers, which can contribute to extending the lifespan of products in accordance with the objectives of the circular economy.

- **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 be 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.
- **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 data are protected. Further to this, BEUC considers 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.
- **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.
- **Adopt technical solutions such as Information Management Systems (PIMS) 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)²⁷, 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.
- **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

²⁷ 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

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 time 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 EU Directive on representative actions should ensure that consumer organisations can represent consumers in such circumstances.

- Reduce the risks of data concentration and excessive data collection: 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.
- 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"²⁸. 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 Policy²⁹. 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).

²⁸ 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) *OJL 321, 17.12.2018, p. 1–35*

²⁹ 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>