The Consumer Voice in Europe

A EUROPEAN STRATEGY FOR DATA

BEUC's response to public consultation

Contact: Agustín 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-2020-046 - 05/06/2020

Why it matters to consumers

In an increasingly digitalised economy, data is an indispensable input for the development of innovative products and services. However, consumers often cannot 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 societal-valuable innovation. Determining who has access to data, including consumers' personal data and under which circumstances and conditions it can be used are key elements for achieving the objective of a healthy and competitive digital economy that delivers benefits to consumers.

Summary

This paper provides BEUC's views on the Commission's Communication "A European strategy for data" addressing key question of the public consultation.

BEUC welcomes the Commission's human-centric approach of its strategy. In the European Union, the processing of personal data has a fundamental rights dimension since personal data and privacy are protected by the EU Charter of Fundamental Rights. Therefore, EU policies must be guided by and designed to ensure the effective implementation of these rights as well as striking a fair balance with other fundamental rights protected by the EU Charter. In this sense, BEUC would like to highlight the following elements of the strategy and consultation:

- *While data can have economic value, it is important to legally distinguish between personal and non-personal data. Access to personal data is subject to mandatory conditions and rights stemming from the General Data Protection Regulation (GDPR).*
- *Since datasets can combine personal and non-personal data, access to the whole data set should be governed by the rules of the GDPR.*
- *The consumer should always be able to decide who gets access to his or her personal data and under what conditions. Overruling this active role of the consumer should be limited to exceptional cases established in the law.*
- *BEUC welcomes that the European Commission is proposing to adopt measures in the Data Strategy to empower individuals to exercise their data protection and privacy rights more effectively, including the Commission plans to adopt measures to enhance the portability right under Article 20 of the GDPR in its upcoming Data Act.*
- *Competent authorities must be able to scrutinise the governance of sectoral data sharing initiatives to ensure compliance with consumer, competition and data protection rules.*
- *Finally, BEUC calls on the Commission to be cautious about enabling data access for public interest purposes in a way that can lead to liberating data collectors from their obligations stemming from the new consumer law Directives or the GDPR.*

General remarks

BEUC welcomes the Commission's Communication "A European strategy for data"[1]. This strategy outlines important measures to be undertaken by the European Commission to ensure the data economy works for consumers. In particular, BEUC welcomes the Commission's human-centric approach and the need to uphold European values and fundamental rights in its data policies. This paper provides BEUC's input to the Commission' consultation on the European Data strategy.

Data is part of a new economic and social order. Companies see data as a crucial input for product development, optimisation of production and the take-up of new technologies such as artificial intelligence. At the same time, data can influence how public bodies design and implement public policies and, ultimately, how consumers are able to enjoy the benefits of digital technologies and the Internet of Things (IoT) in a non-discriminatory, safe and secure manner. Digitisation has brought, and has the potential to bring even more, benefits to consumers and to society at large. Still, it has also raised new concerns stemming from the collection, aggregation and use of data from consumers[2].

In the European Union, the processing of personal data has a fundamental rights dimension since personal data and privacy are protected by the EU Charter of Fundamental Rights. Therefore, EU policies must be guided by and designed to ensure the effective implementation of these rights as well as striking a fair balance with other fundamental rights protected by the EU Charter. This balancing exercise raises sensitive issues about the extent to which personal data can be subject to market dynamics.

1.1. A (single) market for data?

While data can have economic value, it is important to distinguish between personal and non-personal data. When it comes to non-personal data, the commercialisation of such data between firms is already done under licenses and contracts.

Regarding personal data, the situation is more complex because it is not regulated as a proprietary right. Protection of personal data in the EU is a fundamental right subject to enforceable mandatory conditions and rights stemming from the General Data Protection Regulation (GDPR)[3]. Hence, companies and organisations cannot dispose freely of consumers' personal information is the same way as tradable goods.

Therefore, when talking about the creation of a single market for data, we must acknowledge that personal data is not subject to the same rules as goods and services. Quite the contrary, protection of personal data as a fundamental right imposes necessary restrictions on the collection, use and sharing of personal data. This of course does not mean that personal data has no economic value or that cannot be protected by other areas of law such as consumer laws. As indicated in a ruling by the Regional Administrative Court of Lazio (*Tribunale Amministrativo Regionale del Lazio - Roma*)[4] personal data is subject to economic exploitation and that is why it can be considered as a counter-performance in seemingly free services like social networks. However, from BEUC's perspective this cannot be understood as meaning that personal data can be treated like any other good subject to the rules and customs of commerce. Further to this, in the aforementioned case, the court ruled that the fact of deriving economic value from consumers' data required the trader (Facebook) to correctly inform consumers that data harvested from consumers

[1] COM(2020) 66final, 19.02.2020.
[2] See in this regard BEUC's position paper, "Access to consumer data in the digital economy", Ref.: https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf (accessed on 31/05/2020).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[4] Tar Lazio, Roma, Sez.I, Judg. 00260/2020 and 00261/2020 published on 10 January 2020.

would be used for commercial purposes beyond the use of social networks. Failing to disclose this was deemed a deceptive practice.

1.2. Data for the common good

Personal and non-personal data can serve the common good. Access to data can enable governments, agencies and non-governmental organisations like consumer groups to fulfil their mandates more efficiently and develop services to benefit of consumers. Examples from consumer organisations include services developed by our Belgian member Test-Achats to monitor mobile coverage in Belgium and help consumers to pick the best service provider in their region[5], and the applications developed by our French and Danish members, UFC-Que Choisir and Forbrugerrådet Tænk respectively, to help consumers identify dangerous substances in cosmetics[6] and other products[7].

Non-personal data can be held by both private and public entities. For data held by public entities, the recently revised Public Sector Information Directive[8] provides the legal basis for making data from publicly-funded services widely and freely available. This is a step in the right direction, which will enable a wide range of actors to access non-personal data necessary to develop new services of common interest and value. Enabling access to such data held by public entities is in line with the spirit of the right to freedom of information of the EU Charter. When it comes to non-personal data held by private entities, the ongoing work of the European Commission on business-to-government data sharing should shed some light on the conditions under which private companies should be required to share non-personal data with governments.

Against this background, it is also important to explore the sharing of non-personal data held by private companies with non-governmental organisations, like consumer organisations, for example with the purpose of improving the testing of products and enforcement. Organisations pursuing public interest objectives should have access to non-personal data to strengthen their actions. This will be very important for stepping up their role as market watchdogs since data can reveal systemic problems and market patterns. Furthermore, the use of data and AI-based instruments for enforcement will bring new opportunities for enforcement agencies. This is recognised by the Commission in its Single Market Enforcement Action Plan[9]. The creation of a "*laboratory (e-enforcement lab) funded under the single market programme would allow testing and application of advanced IT solutions using big data techniques and AI. Given the relevance of this for a broad range of EU rules, the Commission will explore whether this laboratory can be integrated into or linked to existing structures, such as the CPC network (…)*".

Regarding personal data, BEUC would like to call for a cautious approach. The consumer should always be able to decide who gets access to his or her personal data and under what conditions. Overruling this active role of the consumer should be limited to exceptional cases established in the law. It would be inappropriate to allow public authorities or private entities to make "non-commercial" use of consumers' personal data under the guise of it being a "common good" in a way that is incompatible with the GDPR.

1.3. Data sharing by consumers

Consumers provide and generate huge amounts of personal information through the use of IoT devices and digital services. This data, when aggregated, has considerable value for businesses which can use it to develop and provide new services, as well as to gain a competitive advantage over rivals that do not have access to the same amount of data, or

[5] Ref.: https://www.test-achats.be/hightech/gsm/calculateur/carte-de-la-couverture-du-reseau-mobile (accessed on 31/05/2020).
[6] Ref.: https://www.quechoisir.org/application-mobile-quelcosmetic-n52804/ (accessed on 31/05/2020).
[7] Ref.: https://kemi.taenk.dk/english (accessed on 31/05/2020)
[8] 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
[9] COM(2020) 94 final, 10.03.2020.

face barriers in accessing data directly from consumers due to the presence of intermediaries (e.g. when data is essential to provide after-sales services as is the case in the automobile sector).

For consumers, it is most of the time very difficult to control the flows of their personal information. They do not know with whom firms are sharing their personal data and for what purposes, even if this is described in the privacy policies of some (but not all) companies. These policies are often dressed up in obscure language and are too lengthy and complicated to be informative, as demonstrated by the research carried out by our Norwegian member on terms and conditions of apps[10]. Reading and understanding privacy policies it is not amongst consumers' priorities in life as these are designed by and for lawyers, not for consumers. In many cases these policies are deliberately vague and do not allow the consumers to understand how her personal data will be exploited. Therefore, **BEUC welcomes that the European Commission is proposing to adopt measures in the Data Strategy to empower individuals to exercise their data protection and privacy rights more effectively**. Indeed, the absence of convenient technical tools to manage data access permissions and control flows of personal data often renders data subjects' rights under the GDPR ineffective[11].

However, we would like to stress that **these measures need to be accompanied by strong and consistent enforcement of the GDPR throughout the EU**. It would be inappropriate to put the burden of controlling complex data flows on the shoulders of consumers alone. Data protection enforcers must ensure that companies comply with the GDPR in its entirety. This means ensuring that companies not only have the appropriate legal basis for processing personal data but also respect the principles enshrined in the GDPR, including the principles of data minimisation, and data protection by design and by default.

Furthermore, to ensure that data sharing works efficiently, the EU should address the limitations of the data portability right under Article 20 of the GDPR:

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 behaviour[12]. 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 service[13].

In a similar vein, the Free Flow of Data Regulation in Article 6 also deals with the portability of non-personal data between firms but it does not tackle market failures stemming from refusal to grant access to data by an incumbent, since it relies on self-regulation without

[10] Ref.: https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/ (accessed on 31/05/2020).

[11] EDPS opinion on "Personal Information Management Systems - Towards more user empowerment in managing and processing personal data", Ref.: https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en (accessed on 31/05/2020).

[12] 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.

[13] 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.

assigning any data access right to third-parties or safeguards. Such is the case when a company refuses to grant access to data that can be considered indispensable because it cannot be obtained through other means or points of access (e.g. access to data stored in a product to perform a repair or maintenance).

Therefore, **BEUC welcomes that the Commission plans to adopt measures to enhance the portability right under Article 20 of the GDPR in its upcoming Data Act**.

1.4. Data spaces

The Commission's strategy proposes the creation of nine data spaces which are domain-specific and cover different industries. Without providing detailed comments on each space at this stage, BEUC would like to highlight that **a sector-specific approach to data access seems to be more appropriate as it allows targeting specific solutions taking due account of existing bottlenecks for data access and market failures of each sector**. In this sense, sector-specific legislation can be used to tackle market failures in a more precise manner while at the same time allowing the adoption of strong safeguards to protect consumers.

Data governance

The effectiveness of a data sharing ecosystem depends on its governance. If data access is only managed by an incumbent data holder, it is likely that those seeking to get access to the data will face barriers. We have seen this in the automobile sector. Car manufacturers were able to dictate the conditions for parties to access in-vehicle data which are less favourable than the conditions applied to the car manufacturers themselves. This is because the economic incentives to keep the data for themselves, in order to provide exclusive services to consumers and apply monopoly prices, outweigh the benefits of licensing that data to third parties[14]. This is one of the reasons the European Union intervened by imposing, in the Type Approval Regulation[15], mandatory access to data necessary in the after-market for repair and maintenance. This shows why, without a clear legal framework, it would be difficult to set up a governance model where the different parties concerned were able to have a voice in the data sharing process. Independently of the technological model chosen, certified market players should have access to the same data quality, latency and granularity which is technologically possible under fair and non-discriminatory terms and fulfilling the conditions set out in the GDPR and other relevant legislation.

When it comes to the sharing of consumers' personal data, any governance scheme needs to take account of the position of consumers vis-à-vis the entities seeking to gain access to their data. In our position paper " Access to consumers' data in the digital economy", we provided a list of criteria for the adoption of data access regimes, including: 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; 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 and consumers must have access to redress when these principles are not respected.

[14] See BEUC letter to Commissioners Vestager and Bulc, Ref.: https://www.beuc.eu/publications/beuc-x-2019-058_letter_to_commissioner_vestager.pdf (accessed on 31/05/2020).
[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, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

In addition to that, it is important that the competent authorities are able to participate in the governance of sectoral initiatives to ensure compliance with the data protection and privacy rules. This can be done by a) allowing Data Protection Authorities (DPAs) to take part in the governance scheme if sharing data in a business-to-government context and b) by being consulted e.g. in the context of sectoral codes of conduct to be validated by a DPA when the scheme is run by private entities under Article 40 GDPR. Further to this, it would be also important that competition agencies remain vigilant should the sharing of competitively sensitive data between companies in the context of private initiatives lead to an eventual harmful coordination between competitors prohibited under Article 101 TFEU.

2.1. Standardisation, interoperability and access to APIs

Lack of access to standardised data and interoperability between services can be an important barrier to enabling data sharing and stimulating competition between companies to the benefit of consumers. Data access and interoperability can be mandated by law or be required by a decision of a competition authority when it is needed to tackle specific market failures stemming from lock-in effects and refusal to grant access to data enabling others to provide innovative products to consumers and compete on the merits. These measures should be proportionate and competition-orientated while maintaining the incentives of *de facto* data holders to innovate in a way that benefits consumers. This means that data sharing must be targeted and serve to a specific purpose and not become an end in itself, for example, when market players call for data reciprocity with the sole objective to gain access to the consumers' data held by tech companies.

As we have seen in the context of open banking, a legislative intervention proved necessary to introduce competition between banks and third-party service providers so as to open the market for payment services and account information services to newcomers. However, more needs to be done to ensure consumers' data is well protected. This is why BEUC calls for standardisation of a unique and single EU-wide Application Programming Interface (API) to be elaborated by a standardisation organisation[16].

2.2. Secondary use of consumers' data

The Commission asks whether data, including health data, could be re-used for public interest. Indeed, public authorities could do more to make data available for R&D purposes provided that data does not allow the identification of individuals, in which case the GDPR would apply. It is worth noting that the EDPB has provided guidance about how the GDPR applies in the context of medical research involving personal data related to an individual's health status thus the re-use of data is already covered and the Commission should take as a basis the work already done[17].

If public bodies make available data for research purposes, it would be only appropriate that there are conditions attached to the sharing of this data if the research would ultimately be exploited commercially as a result of the development of medicines and treatments. Therefore, BEUC recommends that, when this non-personal data is shared with companies engaging in R&D, relevant agreements between public entities and such firms should include conditions such as allowing third parties to access and use the research

[16] See BEUC letter to Vice-President Dombrovskis, Ref. https://www.beuc.eu/publications/beuc-x-2017-054_mgo_psd2_-_secure_communication_between_banks_and_third_party_psps.pdf (accessed on 31/05/2020).

[17] See in this regard: EDPB's Opinion on the interplay of the Clinical Trials Regulation and the GDPR: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf ; EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak: Ref.: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en (accessed on 31/05/2020).

results on fair and reasonable terms. In addition, non-personal data sharing in the form of open data initiatives should be stimulated[18].

Data "altruism"

The Commission's consultation asks whether law and technology should enable citizens to make available data for public interest purposes without direct reward. In essence, what the Commission wants to know is whether consumers can "donate" their personal data. From a data protection perspective, nothing prevents consumers from allowing data controllers to use their personal data for public interest purposes provided that there is a) a legal basis for the processing of the data and b) that the processing respects the obligations and principles set out in the GDPR.

However, BEUC would like to highlight that the term "data altruism" is a problematic label with unclear consequences for data subjects, for example, to differentiate genuine from manipulative data donation campaigns and initiatives. It implies nudging consumers into "ethical" behaviour, which – depending on the specific case may not be justified. Moreover, since **the concept of data altruism does not exist in EU or national law**, the Commission should avoid using this term as it risks creating the wrong perception that making available data for public interest purposes is unregulated while in reality this is covered by the GDPR.

The Commission's question includes two elements which must be treated separately, first the definition of what a public interest purpose is, and secondly what we should understand as direct reward. Finally, this section analyses two public-interest purposes considered by the Commission: health research and mobility.

3.1. Public interest purpose as a basis for data donation

There is no uniform concept of public interest in EU law. Under the GDPR, public interest purposes are implied in Article 6(1)(e) regarding data that is necessary for *"the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller"*. Here it is important to highlight that this legal basis concerns controllers who perform a specific task in the public interest and who exercise official authority set out in law, as defined by a Union or Member State law as indicated in recital 45 GDPR: *"it should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association."* Unfortunately, there is no provision in the GDPR defining what constitutes a public interest activity independently of who carries out the activity.

Therefore, it would be necessary to have **a common understanding of what constitute public interest activities and the criteria to establish when data donation is done for public interest purposes**, as a safeguard to prevent situations in which consumers willingly give away their data under the mistaken belief that it was done for good reasons while in reality their data is exploited commercially ("data-altruism washing"). This deceptive situation could be addressed using the existing framework of the Unfair Commercial Practices Directive: if an economic operator (e.g. a health facility) were to advertise its involvement in research along with the opportunity for its patients to authorise

[18] An example of this is the COVID19 Data Portal initiative, Ref.: https://www.covid19dataportal.org/ (accessed on 31/05/2020).

the use of their personal data as a contribution in the public interest, any failure to disclose the exact terms of use of such data could be deemed as a misleading market practice under Article 6.

3.2. No direct reward

The second element of the question relates to whether consumers should *not* be rewarded for making available their data. However, it is not clear what 'reward' means in this context. From a contract law perspective, it can be understood as a counter-performance, consisting in a monetary payment or another form of remuneration e.g. such as access to a digital service or digital content. It is worth highlighting that under the recently adopted Digital Content and Digital Services Directive[19], allowing the collection of personal data is considered as a counter-performance for accessing digital services or digital content although it is not a price in the traditional sense in line of the considerations expressed above. This Directive made an important step in EU consumer law by acknowledging that consumers accessing such services as a result of the provision of personal data merits being protected. This is also the case in the new Omnibus Directive[20] updating the scope of the Consumer Rights Directive[21].

Against this background, the Commission must be cautious about enabling data access for public interest purposes in a way that can lead to liberating data collectors from their obligations stemming from the new consumer law Directives or the GDPR. **From BEUC's viewpoint both the GDPR and the consumer rights under the new Digital Content and Digital Services directive must be fully applicable.** It would be very easy for a company to make consumers believe that the data they provided would be used for public interest purposes when the opposite might be true therefore depriving consumers of a counter-performance in line with the Digital Content and Digital Services Directive and exposing them to unfair data practices and discrimination stemming from targeting and profiling[22]. Especially when such profiles can be used to establish individual consumers' willingness to pay and therefore capture more value from them in the form of personal prices[23], deny access to services or reduce their choices.

3.3. Public interest purposes related to health research and mobility

The Commission suggests two specific purposes for making data available without reward: health research and aspects related to a city, municipality or region including improving mobility and environmental change that can be addressed locally.

First regarding health research, while there might be merits to allowing consumers to permit the processing of their data for health research purposes, we cannot forget that this situation is regulated in the GDPR under Article 9 on the processing of special categories of data. Thus, any data sharing for research purposes must comply with the special regime of the GDPR. Further to this, we would like to highlight that if consumers were to make data available for health research, this should not be for commercial purposes and if the

[19] 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.
[20] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.
[21] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.
[22] The report of the Norwegian Consumer Council "Out of Control" provides for examples about how easy is to mislead consumers through the presentation of privacy choice creating the false perception of control when in reality the design of interface features seek to keep consumers sharing personal data, which is at odds with data protection and privacy rights, Ref.: https://www.forbrukerradet.no/out-of-control/ (accessed on 31/05/2020).
[23] See BEUC note to the OECD, "Personalised pricing in the digital era", Ref.: https://one.oecd.org/document/DAF/COMP/WD(2018)129/en/pdf (accessed on 31/05/2020).

outcome of the research then contributed to the development of medicines and treatments that were exploited commercially, conditionalities should apply e.g. enabling the research data to be used by other parties and not licenced on an exclusive basis. Consumers should be also protected against misleading practices regarding initiatives by the industry which are presented as public purpose research when in reality there is a commercial intent in the exploitation of the data as a result of the commercialisation of the research outputs.

Secondly, concerning data processing to improve mobility aspects of a city, municipality or region, since much of this data is used by public authorities, the collection and processing of data for these purposes would already be covered by the GDPR as outlined above. Should these data be collected and processed by private parties not qualifying for the legal basis for collection stipulated in Article 6(1)(e), then the collection needs to take place using the other legal basis (i.e. consent) and be carried out within the limits of the GDPR.

Data intermediaries

The digital economy has paved the way for the emergence of data intermediaries that act as brokers between different actors. The most developed sector is the ad-tech industry. However, research by consumer organisations has highlighted serious concerns about the compliance of these actors with privacy, data protection and consumer laws. Therefore, BEUC calls for caution on stimulating the development of data intermediaries without first, by efficient and strong enforcement of existing rules, solving the problems in the current business models based on the exploitation of consumers' data.

Consumer organisations can contribute by empowering consumers to rebalancing the digital ecosystem characterised by the presence of incumbents which control and dictate what innovation reach consumers. This can be done for example by making sure that the innovation developed with consumer data is actually consumer-centric and creates real value back for consumers. Further to this, consumer organisations can help consumers navigate in digital markets by providing independent advice about the trustworthiness of the companies accessing and using their data (e.g. checking legal compliance, existence of security measures, etc.). However, this must be accompanied by strong enforcement of the existing rules.

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