The Consumer Voice in Europe

GIVING CONSUMERS CONTROL OF THEIR DATA

BEUC position paper on the Data Act proposal

Contact: Kasper Drążewski and Maryant Fernández - 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-2022-103 - 07/10/2022

Why it matters for consumers

Consumer use of connected products, from smart vacuum cleaners to connected cars, generates immense amounts of data. Who can access this data and what it can be used for has important implications. Access to the data, or lack of it, can mean the difference between consumers having to pay more at a car dealership or having the option to go for a third-party repair venue on the corner that is potentially cheaper. Putting consumers in control, by empowering them to decide who to share their data with, can deliver greater and better product functionalities and services to consumers, thereby favouring innovation that benefits consumers. However, without the right protections which need to be added to the Data Act, consumers risk becoming subject to more complex, burdensome and unfair terms in contracts and pushed to grant full access to data generated by some of their devices to countless third parties for opaque purposes.

Summary

The Data Act aims to respond to the challenge of enabling healthy competition, meaningful innovation and consumer data control. However, the proposal by the European Commission, while taking a step in the right direction, falls short of achieving this objective and needs substantive improvements.

The proposal *de facto* puts data holders into a position of 'owners' of data, turning them into gatekeepers of the data generated by the products they sell. This leaves little space for the 'meaningful control' the Act promises to users. The draft Data Act generally treats consumers in the same way as business users, which means consumers are not sufficiently protected. Transparency seems to be the main means of protection and dark patterns are only prohibited when used by third parties, not data holders. Mandating extensive pre-contractual disclosure cannot be the only means to enable consumers to control the data generated.

BEUC's recommendations to address the most urgent concerns:

1. The definitions in the Data Act need further work to be comprehensive and coherent with other EU laws such as the General Data Protection Regulation.
2. Consumers must be protected by design and by default. Notably, certain contractual clauses should be prohibited for B2C contracts, such as bundling necessary and unnecessary purposes of processing. The Data Act should not only prohibit the use of dark patterns by third parties, but also by data holders.
3. Consumers must be in control of data generated through the use of products and related services. This for instance requires meaningful consumer choices according to their preferences and an enhanced data portability right with clear format and interoperability conditions.
4. The Data Act must promote competition and a healthy data economy. BEUC welcomes that the Data Act restricts access to data for gatekeepers, but the role of data holders should be more carefully designed so they do not monopolise access to data.
5. The Data Act must ensure swift and effective redress and enforcement. This for example requires a formal cooperation mechanism between data protection authorities and other competent authorities.

Further recommendations:

1. **Key definitions in Article 2 and related recitals must be amended.** In particular:
    - Definitions must be coherent with other related EU laws, including the General Data Protection Regulation, the Data Governance Act and the ePrivacy Directive.
    - The definition of 'users' does not distinguish between consumers and corporate users of products. The proposal should therefore introduce a definition of 'consumer' in line with the consumer law acquis. This will allow for tailored protection for consumers when they purchase products or decide on their data being shared.
    - The concept of 'user' should cover consumers that use a product without being the owner, renter or leaser of a product. Otherwise, individuals using a connected product do not have data rights under the Data Act.
    - Exclusions from the definition of 'product' should be explained and duly justified as the rationale for the distinction is not clear and there is a mismatch between the definition in Article 2(2) and the examples provided in recitals 14 and 15.
    - The definition of 'data' should include data that is processed using the device's own computing capacity.

2. **Consumers must be protected by design and by default.** Notably:
    - Data processing should depend on consumers' choice according to their preferences and differentiating between data that is essential for the functioning of the device and other types of data (Article 3).
    - 'Dark patterns' used by both data holders (Article 3) and third parties (Article 6 (2) (a)) should be prohibited. The wording should be aligned with that in Article 13 (6) of the Digital Markets Act.
    - Like third parties (in Article 6 (2) (b)), data holders (in Article 3) should not process data for profiling purposes except if profiling is strictly necessary for a specific service explicitly requested by the consumer.
    - Article 1 should ensure that the Data Act does not affect the applicability of EU consumer protection laws, including the Unfair Commercial Practices Directive and the Unfair Contract Terms Directive.
    - There must be a list of prohibited contractual clauses for B2C contracts ('blacklist'), such as bundling necessary and unnecessary purposes of data processing together.
    - The exception for small and micro-enterprises in Article 7(1) should be deleted. Otherwise, virtually none of the consumer benefits under the proposed Data Act would apply if the device were made, or the service were performed, by a micro- or small enterprise. Consumers should be protected and empowered regardless of the company's size that they are dealing with.

3. **Consumers must be in control of data generated through the use of products and related services.** This requires the following:
    - Article 1(3) should state that in case of conflicting provisions European data protection and privacy legislation should prevail.
    - Under Article 3 users should have the right to obtain a copy of the data similarly to Article 15 GDPR.
    - Use of a connected product offline must be ensured under Article 3 if that can be reasonably expected due to the nature of the product.

- An enhanced data portability right under Article 5, with a broad scope and specific interoperability and format requirements, so it is much easier to exercise than it is today in the GDPR.
- Data sharing to be truly free of charge for consumers. Consumers cannot be asked indirectly to pay to not being locked in by data holders and they should be allowed to directly share data with third parties (Article 9).
- Consumers who wish for a third party to access their device's data should not have to be involved in subsequent negotiations between the data holder and the third party about the specifics of this process (e.g., the types of data needed for a given purpose, how and in which format the data should be made available) as this would be too burdensome (Articles 6 (1), 8 (2)).
- If the processing of personal data made available to a data recipient pursuant to Article 5 is restricted in line with Article 6 of the Data Act, these provisions should take precedence over Article 6 GDPR.
- The Data Act to not establish new purposes for processing personal data on top of the GDPR regime. Instead, it should only enable personal data to be used for specific purposes, such as aftermarket services or other narrowly defined "value added services" with consumers' consent.
- A granular data processing consent structure that is applicable to all users.
- The GDPR must apply in full to mixed datasets in line with the Free Flow of Non-personal Data Regulation.
- Consumers' data to be effectively anonymised to qualify as non-personal data. Otherwise, non-personal data could become personally identifiable for example via cross-referencing with other data or other forms of de-anonymisation.

4. **The Data Act must promote competition and a healthy data economy.** In particular:
    - Data holders should not become gatekeepers of the data generated by products. Therefore, data holders should only be able to prevent use or disclosure of data when data constitutes a narrowly defined trade secret (Article 11). Monitoring data interactions between users and third parties should only be permitted for objectively justified security considerations (Article 5 (5)).
    - Safeguards to prevent further accumulation and exploitation of data by gatekeeper companies are essential (notably Articles 4 (4), 5 (2), 6 (2)). These types of safeguards were key components in the Digital Markets Act and they should also apply to the Data Act.

5. **The Data Act must ensure swift and effective redress and enforcement:**
    - Consumers need effective remedies and redress mechanisms if their rights are not respected. We welcome that the Data Act would be added to the annex of both the Representative Actions Directive (Article 37) and the Consumer Protection Cooperation Regulation (Article 36).
    - Enforcement by competent authorities and cooperation between them needs further details (for example on how to handle a complaint, applicable deadlines) not to repeat the same mistakes of the GDPR and other EU laws.
    - There must be a detailed cooperation mechanism between data protection authorities and other competent authorities.
    - There must be harmonised minimum penalties for infringements other than those set forth in Article 33 (3) and (4) to avoid forum and enforcement shopping across the EU.

Table of Contents

1. Introduction

Connected devices are already everywhere. Smart driver assistance systems on cars can make driving easier and safer; smart thermostats can help conserve energy and reduce bills; robot vacuum cleaners can save us a lot of time and effort with our household chores. By using these types of products every day, the modern-day consumer uses and produces increasing amounts of data – both personal and non-personal. What can be done with this data and by whom, however, is a complex issue, particularly from a consumer perspective.

BEUC welcomes the Data Act proposal[1] as a bold initiative aiming to respond to the challenge of enabling healthy competition, innovation and consumer data control.

[1] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data, COM(2022) 68 final 2022/0047 (COD).

However, we have identified several shortcomings. Throughout this paper, we propose recommendations to address them. Many of the elements of the Data Act proposal that we either welcome or find problematic also appear in the recitals. We urge policymakers not to neglect the recitals and to reinforce the body of the proposal.

2. Definitions and concepts in need of clarification

The Data Act proposal puts forward an ambitious framework meant to facilitate circulation of data, prevent vendor lock-in for users of connected devices and cloud services, and ensure healthy competition and innovation that benefits consumers. The efficiency of the system and its application will strongly depend on how the main elements of this system are defined and whether proper safeguards are in place.

2.1. User

Article 2 (5) defines 'user' as a "natural or legal person that owns, rents or leases a product or receives a service". The definition does not allow for tailored protection of consumers as the definition covers both individuals and companies. Having specific provisions to protect consumers is particularly important to safeguard vulnerable consumers, such as the elderly or very young consumers. At the same time, the definition is not tied to actual use of a product. Therefore, an individual who is just using somebody else's product (such as driving a borrowed or company-owned vehicle) has no rights under the Data Act proposal.

Incidentally, an individual as a data subject only benefits from the framework of the Data Act depending on their legal relationship with the product or the related service rather than on their relationship with the information concerning their private use of the product or service.[2]

Finally, the proposal's definition of 'user' is specific to the Act and differs for example from the understanding in Article 2 a) of the ePrivacy Directive[3] which denotes a natural person using a publicly available electronic communications service.

BEUC recommendations

- The Data Act should add a **definition of 'consumer'** which follows the Consumer Rights Directive to allow a tailored protection of consumers.
- To ensure personal data rights are not undermined by the Data Act and cover data subjects whenever relevant, for example to exercise their data portability right, the term **'data subject' should be added** to the term 'user' in relevant provisions of the Data Act, notably in Chapter II.
- A new first paragraph should be added to Article 2 to avoid confusion and **ensure the definitions of the General Data Protection Regulation (GDPR)[4] apply**[5].

[2] This has also been pointed out by the EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).
[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy Directive).
[4] 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, 'GDPR').
[5] This would e.g., serve as an indication where the user may also be the data subject. An alternative recommendation was offered in the EDPB-EDPS Opinion postulating for the Data Act to clearly differentiate the situations where the user is the data subject from the situation where the user is not the data subject (para. 39).

- Article 2(5) and recital 18 should be amended to ensure that the **concept of 'user' covers individuals who use a product without being the owner, renter or leaser of the product.**
- To minimise the risk of misinterpretation and ensure legal certainty, the Data Act should also include a **recital explaining the relationship between its definition of 'user' and that used in the ePrivacy Directive.**

2.2. Product

In Article 2 (2), the proposal defines a 'product' as a tangible, movable item that:

a) "obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and"

b) "whose primary function is not the storing and processing of data".

This distinction raises the question as to whether certain products fall within the scope of 'product' or not. According to Recital 14, products such as "vehicles, home equipment and consumer goods, medical and health devices, or agricultural and industrial machinery" would be included. However, "personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners" would be excluded from the scope (Recital 15).

When checking these examples against the proposed definition of product, we fail to understand the rationale behind the distinction. For example, the primary function of a fitness tracker is to process and store data;[6] similarly, the distinction between a smartwatch and a smartphone may not be clear enough to justify different treatment under the Regulation. Also, a smart TV is a device "primarily designed to display or play content" which would suggest it should not be considered a product under Recital 15, despite its primary function not being that to store and process data.

We conclude there is a fundamental problem in what falls under the exclusions and what doesn't. For example, it is unclear whether virtual assistants or smartwatches would be included or not. It is possible that the distinction lies in whether the human input amounts to the creation of 'content'. Content, however, is not defined in the proposal.

BEUC recommendations

- The Data Act's **removal of certain consumer products from the scope should be clearly explained and justified** in a recital. If the ability to record or store content is to be used as a basis for distinction between what constitutes a product and what does not, at minimum, 'content' should be defined in Article 2 of the proposal.

2.3. Data

The definition of data in Article 2 (1), which is crucial to the Data Act, speaks of "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording". In the context of data portability, the scope is defined more broadly than in Article 20 GDPR as it also expressly includes 'observed data' rather than just data that is actively provided (Recital 31).

[6] Processing under the GDPR entails collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 para. 2 GDPR).

Data generated by the use of a product or related service include:

- data recorded intentionally by the user,
- generated as a by-product of the user's action, such as diagnostics data, and
- generated without any action by the user, such as when the product is in 'standby mode',
- recorded during periods when the product is switched off (Recital 17).

The scope of 'data' under the proposal excludes data that is inferred or derived from the data categories listed above (Recital 14), in particular data resulting from any software process that calculates derivative data (Recital 17).

In the context of the data sharing rights, it is thus important that only user-recorded or user-created data and raw data can be shared with third parties. Any algorithmically-processed data (with no distinction of whether it is processed in-device or by the data holder) is explicitly excluded from scope.

From the perspective of consumers, this can lead to difficulties in benefiting from the data portability rights under this Regulation. For example, a connected device may be difficult to diagnose and repair if access is only given to the raw data its sensors collected – rather than enabling a full analysis of how it processed this data internally at the time of malfunction.[7]

BEUC recommendations

- To ensure that the framework of the Data Act meets its objectives, the definition of **'data'** should be broadened as it should **not exclude data that has been processed using the device's own computing capacity** (for example, the history of automated braking events in a connected car). This should be an exception from the exclusion of derivative and inferred data from the scope of the Act under Recitals 14 and 17.
- A recital should make clear that the principles of **data minimisation and data protection by design and default** set forth under the GDPR apply. This will ensure that the processing of personal data in a distributed and more privacy-friendly way would not be discouraged or deterred.

2.4. Data holder and data recipient

The proposal defines the data holder as an individual or an organisation (a "legal or natural person") legally obliged or authorised to share certain data. This may be combined with an *ability* to share it, provided the data is non-personal and the data holder is in control of the technical design of the product and related services.

'Data recipient' is defined as a legal or natural person acting for business purposes, who is not the user, and to whom data is made available by the data holder, on the basis of Union or national legislation or following a request by the user. The term is often used interchangeably with 'third party' (e.g., Chapter 2 refers exclusively to 'third parties').

Notably, the proposal does not explain how these terms relate to the terminology of the GDPR or the Data Governance Act (DGA)[8] concerning personal data, in particular the

[7] On this matter, see also Drexl, Banda et al. (2022) Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022, p. 10, para. 24 *et seq*.
[8] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act, 'DGA').

notions of 'data controller' and 'data subject' which may lead to confusion in their interpretation and use.[9]

BEUC recommendation

- To minimise the risk of misinterpretation and ensure legal certainty, the Data Act should ensure the **terms** it uses and those used in **the GDPR and the DGA** are **coherent**.

2.5. Related service

In Article 2 (3), the proposal defines 'related service' as a digital service, including software, which is incorporated in, or interconnected with, a product in such a way that its absence would prevent the product from performing one of its functions. In other words, a 'related service' is a service that is necessary for the full functionality of a product.

It is not clear whether services adding extra functionalities to a product, for example those offered by third parties, can fall within the scope of the definition. This second interpretation seems to be seconded by recital 35 which speaks of a third party using data to develop a "new and innovative product or related service", which may nonetheless be read in two ways:

- Using data for the development of a competing product is not allowed, but it is allowed for developing a competing related service; or
- Using data for the development of a competing product or a competing related service is not allowed. What is allowed is developing a 'new and innovative product' optionally accompanied by a related service.

The first interpretation would have greater benefit from the perspective of fostering innovation, consumer choice and boosting competition.

Lastly, the restriction appears to only apply to third parties. In other words, the user of the device is not expressly prevented from developing competing products or services.

BEUC recommendations

- The wording of Recital 35 should be clarified to expressly **allow the development of related services to existing products using data obtained** under the data sharing provisions of this Regulation.

3. Making consumer protection by design and by default a reality

3.1. Pre-contractual information and data processing by data holders

In the context of IoT devices, consumers find themselves in legal relationships which extend beyond the initial purchase contract in the store or on the website. From the moment of being put into service, a connected device will start generating, sending and receiving data concerning its use. Under Article 3 and Recitals 23 and 24, the basis for this appears to be the purchase contract with the user.

The Data Act proposal relies on disclosure duties, introducing extensive pre-contractual information requirements in Article 3 (2). These include the nature and volume of the data likely to be generated, whether the data is likely to be generated continuously and in real-

[9] For example, article 2 (5) of the Data Governance Act has its own definition of a 'data holder' as a legal person or data subject (emphasis added) who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control.

time, how the user may access this data, who will be using the data, the identity of the data holder, means of mandating third-party access to the data or the user's right to lodge a complaint.

The user is given no say as to what data they agree the device can process. A suggestion aimed at introducing granularity and withdrawal options into interfaces managing data permissions is included in Recital 25, but is only applicable as an exception to markets "characterised by the concentration of a small number of manufacturers supplying end users" where "contractual agreements may be insufficient to achieve the objective of user empowerment". The examples given suggest that this applies mainly to the farming industry, which means that in a consumer situation a 'take it or leave it' contract with the device vendor is deemed sufficient.

An equally important issue is that of obtaining data processing consent through a choice architecture that tricks the user into making undesired choices (dark patterns). Under the draft Data Act, the user benefits from protection against dark patterns when contracting with third parties via a prohibition in Article 6 (2) (a). However, the wording is unfortunately not aligned with that of the recently adopted Article 13 (6) of the Digital Market Act (DMA). By tying a prohibition of dark patterns to 'coercion, deception or manipulation', the Data Act would add new layers of complexity and proof that would not protect consumers. For example, consumers would have to prove intent, which is very difficult to do. Still, under the proposal no protection against dark patterns applies when the user deals with the data holder. Without a clear prohibition of dark patterns in place, even a granular choice architecture will not help.

In addition, the proposal maintains the optic of a weaker protection of users when dealing with data holders in the context of regulating profiling. While third parties are prohibited from using the data for profiling to a certain extent under Article 6 (2) (b), no such protections exist in regard to the data holders.

As a result, the current wording of the Data Act primarily protects the data holders by putting them in a privileged position. Shielded from substantive obligations regarding dark patterns, profiling or granular choice, data holders enjoy significant advantages compared to third parties and users, which includes consumers.

BEUC recommendations

- The disclosure model of consumer protection adopted in the Data Act is insufficient and must be complemented by **protection by design and by default** (see recommendations in Section 3.3 below).
- Consumers must be treated in a way that respects the non-professional nature of their involvement. Under no circumstances should they be treated less favourably than business users operating in certain markets, particularly in terms of having **meaningful choices** on data processing and a right of withdrawal. Mandating an extensive pre-contractual disclosure cannot replace choice. Article 3 (2) should contain a requirement for obtaining consent for data processing that would differentiate between data that is essential for the functioning of the device and other types of data.
- The data holder must always justify the **destination of the data or the purpose for processing** it, not just in case of sharing data with a third party.
- A **prohibition on the use of dark patterns** by data holders should be introduced in Article 3.
- Lastly, Article 3 should **prohibit** use of data processed by data holders for **profiling except if profiling is strictly necessary for a specific service explicitly requested by the consumer**.

3.2. Absence of a fairness-based protection framework for consumers

As the weaker party, the consumer needs regulatory protection that prevents the occurrence of certain unfair and harmful behaviours by traders (ex-ante protection). This approach is in European consumer law, particularly in the prohibitions on unfair commercial practices (where even the reasonable likelihood of harm is sufficient to consider a practice unfair). By contrast, 'ex-post' means of protection, more common in contract law, are based on evaluating cases after a harm has occurred.

The proposal's focus on contracts means it pays little attention to ex-ante consumer protection. A vague reference to consumer law directives is inserted in Recital 9 and in the specific context of contracts between the data holder and the consumer, Recital 26 only mentions the Unfair Contract Terms Directive[10] as being applicable (but not for example the Unfair Commercial Practices Directive[11]). This approach is insufficient because:

- It places the consumer in a classic 'I have read and accepted the terms and conditions' situation. If the consumer then finds that some of the terms could qualify as unfair,[12] they will need to go to court. In practice, since the contract is about collection and use of data, the data will already have been processed by the data holder long ago, leaving little room to reverse the harm after it has occurred.
- The proposed framework is likely to fail under conditions of digital asymmetry where the consumer will not have the resources nor the qualifications to analyse and understand a complicated transparency disclosure.[13]

The Data Act currently is a maximum harmonisation instrument. The sole reference to the UCTD poses the risk of creating a preclusionary effect[14], which prevents the application of other means of consumer protection to user-to-data holder contracts provided by other laws, such as the Unfair Commercial Practices Directive.

In addition, the Digital Content Directive (EU) 2019/770[15] and the Sale of Goods Directive (EU) 2019/771[16] establish requirements to respectively ensure the supply of digital content and services, and the sale of goods (including goods with incorporated digital content or service), conform with the contract.

Under the two Directives, contractual conformity is assessed in two ways: based on subjective criteria (i.e. whether the good or service corresponds with the terms of the contract) and objective criteria (such as fitness for the typical purpose they would be used for, or meeting reasonable expectations for this type of product).[17] If companies fail to

---

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts ('UCTD').
[11] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('UCPD').
[12] Such contract terms, pertaining e.g. to excessive collection or invasive or otherwise harmful uses of data, would need to be assessed by a court of law, under the UCTD's ex post framework of assessing unfairness of contract terms, based on the three criteria, namely (i) being contrary to the requirements of good faith; (ii) causing significant imbalance in the parties' rights and obligations; (iii) this being to the detriment of the consumer.
[13] See BEUC (2022) EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy https://www.beuc.eu/publications/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy/html; Helberger, Micklitz et al. (2021) EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets, https://www.beuc.eu/publications/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy/html.
[14] On the preclusionary effect see Helberger, Micklitz et al. (2021) EU Consumer Protection 2.0. The Regulatory Gap: Consumer protection in the digital economy (2021) https://www.beuc.eu/publications/beuc-x-2021-116_the_regulatory_gap-consumer_protection_in_the_digital_economy.pdf
[15] 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 ('Digital Content Directive', 'DCD').
[16] 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 ('Sale of Goods Directive', 'SGD').
[17] Art. 7 Sale of Goods Directive, Art. 8 Digital Content Directive.

meet these criteria, consumers have the right to seek remedies – unless the company can prove consumers were explicitly made aware and accepted, expressly and separately, that deviation from the sales contract.[18] In other words, the consumer may lose their rights to challenge a non-compliant product or service under the two Directives if they give their consent.

For consumers buying connected devices, particularly given the profound digital asymmetry of knowledge and power that can be expected between consumers and data holders, this optional derogation of consumers' rights by agreement can prove particularly problematic. Studies indicate that in specifically designed online choice environments consent is not difficult to obtain, even when it goes against the preferences of the individual.[19] This type of derogation may easily be used to exclude applicability of consumer remedies and thus negate the consumer protection value of a conformity obligation.

BEUC recommendations

- The model of protecting consumers under the Data Act should not focus on **mandating extensive pre-contractual information** under Article 3. The Act should offer consumer protection by design and by default.
- As for the GDPR and the ePrivacy Directive, Article 1 should ensure that **the Data Act cannot affect the applicability of EU consumer protection laws**, in particular the Unfair Commercial Practices Directive and the Unfair Contract Terms Directive.
- **There must be a black list** of prohibited contractual clauses for B2C contracts in an annex or separate article to curtail excessive collection and harmful uses of data processed through products and services. This black list should *inter alia* include prohibitions on:[20]
    - processing of the personal data generated by the use of a product or service by any data subject other than the user (including use by data holders and third parties) where the data makes it possible to make inferences about private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned;
    - bundling data usage by data holders, for example for purposes both necessary for the operation of the product or the related service together with purposes which are unnecessary, such as use for marketing or development of new products;
    - unrestricted use of personal data generated by the use of a product or related services for purposes such as direct marketing or advertising, credit scoring, to determine eligibility to health insurance or to calculate or modify insurance premiums, among others.
    - Derogating from remedies resulting from non-conformity of a product or a service caused by the trader's breaches of the Data Act.

[18] Art. 7 (5) Sale of Goods Directive, Art. 8 (5) Digital Content Directive.
[19] OECD (2021) The effects of online disclosure about personalised pricing on consumers. ISSN: 20716826 (online) https://doi.org/10.1787/20716826. https://www.oecd-ilibrary.org/science-and-technology/the-effects-of-online-disclosure-about-personalised-pricing-on-consumers_1ce1de63-en. Accessed on 16 May 2022. See also BEUC (2022) EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy https://www.beuc.eu/publications/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy/html; Helberger, Micklitz et al. (2021) EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets, https://www.beuc.eu/publications/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy/html.
[20] Part of this list is based on the recommendations of the EDPB-EDPS joint opinion of 4 May 2022.

3.3. Exception for micro- and small enterprises

Article 7 (1) of the proposal introduces an exception for device manufacturers and service providers who are micro- or small enterprises, who are not partnered up or linked with a larger enterprise, regarding the application of all of Chapter II (including the user's right to access data and to share with third parties, including all the protections against coercive and abusive practices).

In practice, this means that virtually none of the consumer benefits established under the Act apply if the device is made, or the service is performed by a micro- or small enterprise. This is problematic both on grounds of weakening the rules of Chapter II which are embedded in contract and consumer law, particularly the rule of data accessibility by default[21], and in terms of weakening the protection of consumers who may not be aware of this exception for small companies.[22]

BEUC recommendation

- **Article 7 (1) should be deleted.**

4. Consumers must have 'meaningful control' over data and their products

4.1. Relationship with the GDPR and the ePrivacy Directive

The Data Act proposal applies to personal and non-personal data alike without introducing separate regimes and seems to rely on the GDPR framework to ensure protection of personal data. Article 1(3) and Recital 30 stipulate that the Act does not "affect the applicability" of Union law on the protection of personal data, in particular the GDPR and the ePrivacy Directive. However, contrary to Article 1 (3) of the Data Governance Act, it is not explicitly mentioned that **in case of conflicting provisions, European data protection and privacy legislation should prevail.** Similarly, the Data Act does not state that it should not be construed as establishing a legal basis for processing personal data. These considerations are important not to lower the level of protection of data subjects.

BEUC recommendations

- Article 1 (3) should be amended in line with Article 1 (3) of the Data Governance Act.

4.2. Users' right to access device data

The Data Act proposal tackles exclusive control over the use of data generated by connected products or related services which 'typically' lies with the manufacturer or designer of a product or service.[23] The proposed solution is a data access right to empower consumers using products or related services to "meaningfully control" how the data generated by their use of the product or related service is used, while also enabling innovation by more market players.[24]

Article 3 (1) stipulates that the design and manufacture of products, as well as the provision of related services must ensure that the data generated by their use must be "*by default,*

[21] Drexl, Banda et al. (2022) para. 96, p. 35.
[22] Id.
[23] Explanatory Memorandum, p. 13.
[24] *Id.*

easily, securely and, where relevant and appropriate, directly accessible to the user". This availability for access is to be free of charge to the user and in principle ongoing.[25]

Access to data by consumers is to be explained in pre-contractual information (Article 3) but its mechanics are not clearly defined, with no explicit discussion of whether this entails a right to view/save/copy the data for example in case of repair services, the user mandates the holder to share the data with the third party, no mention is made of the user *actually sharing* the data).

This suggests the data holder remains in factual control of the data, supported by the "bringing algorithms to the data" wording of Recital 8 and the data holder "making data available on the product or on their server" provisions of Recital 21.[26]

Furthermore, the product design provisions of Article 3 do not stipulate that the design of products should ensure that a basic set of functionalities is maintained when the product is used offline, in case of products where this would typically be expected (e.g., a smart fridge should still be usable as a fridge without an Internet connection, just as a smart thermostat should still perform its main functions without network access).

BEUC recommendations

- Specific provisions should exist to **clarify the right of the user to obtain a copy of the data similarly to Article 15 GDPR**.
- Where it can be reasonably expected due to the nature of the product, product design provisions under Article 3 should require that **an entirely offline use of a product must be ensured whenever consumers wish to use their product offline.**

4.3. Effective data portability: right to make data accessible to a third party

One of the main benefits of the right to access data for consumers in chapter II is making data available to third parties, such as third-party maintenance and repair service providers. In this sense, BEUC welcomes the intention behind the Data Act to complement and reinforce the portability right included in the GDPR. However, there is a probable area of conflict between the two regimes, regulated in Article 5 of the Data Act and Article 20 of the GDPR respectively. While the proposal rightly recognises the primacy of the GDPR in Article 1 (3), Article 5 (7) and Recital 31, the two regimes are substantially different:

The GDPR's construct is primarily that of a horizontal bilateral arrangement between the data controller and the data subject that allows for a transfer of personal data in a structured, commonly-used and machine-readable format, along with the right to transmit that data to another controller without hindrance from the original controller. Direct transmission between controllers at the request of the data subject is mentioned but only in a recital, not Article 20 itself[27].

The Data Act's framework foresees three parties: the user, the data holder and the third party. The scope of the data is theoretically broader (including non-personal data, as well as observed data) while the data made available is foreseen as a continuous and real-time process (Recital 31, Article 5 (1)). At the same time, a number of limitations may reduce the usability of these provisions. To name the most prominent:

[25] Article 4 (1).
[26] See Section 5.1. for a further discussion in the context of data monopolies.
[27] Recital 68 GDPR states that "[w]here technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another".

- The portability scheme under the Data Act proposal appears to be a temporary arrangement, limited in scope and in time by the purpose for which the data is shared on request of the user and with an explicit requirement for it to be removed by the third party after this purpose has been achieved;[28]
- The scope of the data is reduced by the requirement for it to be only 'raw' data, of which there can be very little (see the discussion and recommendations in Section 2.3 above);
- Although the Explanatory Memorandum recognises their necessity[29], there are no requirements for the data to be in structured, commonly used or machine-readable, not to mention interoperable, formats as under Article 20 GDPR;[30]
- While the data sharing would be free of charge to the user, it would be payable by the third party purportedly as a "reasonable compensation" for the costs incurred and investment required for the data holder to make data available (Article 9). However, the sharing being actually 'free of charge' to the user element is doubtful as nothing in the Act precludes the third party to charge their cost of accessing the data to the user.[31]

In practice, this all means that a consumer seeking to diagnose and repair a robot vacuum cleaner via a third-party repair shop may face a barrage of issues, including an insufficient amount of data or a light scope to it made available, or the data presented in an unusable format. Ultimately, the consumer may also incur significant costs, as the compensation for data sharing owed to the data holder will ultimately be charged to the consumer by the repair shop. As a result, the consumer who has already paid the purchase price for the device will now be required to pay again – this time for the privilege of not being locked-in with the vendor.

Lastly, under Article 6 (1), the user may define the scope of third party use quite flexibly, subject to rights of data subjects and a prohibition of profiling but only where it is not necessary for the provision of the user's requested service.[32] The Data Act thus appears to create too much leeway with regard to the uses of the data, which might also include an incentive to sell one's own data to businesses or intermediaries.[33] This approach would be inconsistent with the understanding expressed in the proposal's Impact Assessment[34].

BEUC recommendations

➢ The Data Act must contain **specific requirements on the modality of sharing and formats of the data** being shared under Article 5, such as those of Article 20 GDPR.

---

[28] Article 6, Recital 35 of the Data Act proposal.
[29] "Data sharing within and between sectors of the economy requires an interoperability framework of procedural and legislative measures to enhance trust and improve efficiency." – Explanatory Memorandum to the Data Act proposal, p. 2. Facilitation of creation of interoperability standards is expressly listed as a specific objective of the proposal (Explanatory Memorandum, p. 3).
[30] Article 20 GDPR on data portability confers upon the data subject the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, with the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
[31] See Drexl, Banda et al. (2022) para. 71 *et seq*.
[32] Article 6 (2) c). See also vzbv (2022) p. 11-12.
[33] Kerber W (2022) Governance of IoT Data: Why the EU Data Act will not fulfil its objectives, Marburg, April 08, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436, p. 10.
[34] Impact assessment report accompanying the Data Act proposal Brussels, 23.2.2022, SWD(2022) 34 final ('Impact Assessment'), p. 153. See also the discussion in Drexl, Banda et al. (2022) p. 10 and vzbv (2022) Verbraucher:innen beim Data Act im Blick behalten: Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act), p. 12.

- The Data Act should ensure that the **rights granted to consumers** under the data access provisions are **indeed** provided to them **free of charge**. The consumer's ability to exercise the rights under the Data Act should not rest on a case-by-case determination of what compensation can be seen as reasonable under Article 9. In return for the fact that the data holder has free access to the user's data, the data holder should release those data to third parties without any costs. In addition, data holders should **allow direct data sharing to third parties by users**.
- To prevent the legitimation and proliferation of privacy-invasive business models, Chapter II of the Data Act should not incentivise, directly or indirectly, **the commercialisation and trade of personal data**.
- **Consumers** who wish for a third party to access their device's data **should not have to be involved in** subsequent negotiations between the data holder and the third party about the **specifics** of this process (e.g., the types of data needed for a given purpose, how and in which format the data should be made available) as this would be too burdensome (Articles 6 (1), 8 (2)).

4.4. Purposes of processing and meaningful consumer choices according to their preferences

While the GDPR allows for using personal data for a different, yet compatible purpose than that for which it was collected,[35] the Data Act prohibits changing the purpose for the processing of the data by third parties.[36] Leaving aside extreme interpretations where non-personal data would be protected more strictly than personal data, this may lead to uncertainty on which of the two regimes should prevail[37] without the Data Act explicitly stating that it establishes a stricter protection regime for data processed by third parties when originating from connected devices. This is because Article 5 of the Data Act proposal creates new possibilities for third parties to process data. However, these should not be unlimited. That is why it is justified for the Data Act to have stricter rules.

Another discrepancy arises with the definition of purposes of processing in a contract between the user and a third party in Article 6 of the proposal. The wording seems to suggest that a contract stipulating the 'agreed purpose' will constitute a standalone basis for processing of personal data by the third party. However, in a profoundly asymmetrical relationship between a consumer and a trader, it is easy to envisage that such a contract may define the purposes of processing quite broadly. This would be allowed under the Data Act but run counter to the GDPR, which requires that processing is carried out for specific, legitimate purposes and limits the use of data on the basis of necessity for the performance of contract.[38]

BEUC recommendations

- The Data Act should clarify the relationship between its provisions and those of the GDPR in relation to the establishment of contracts between users and third parties as legal basis for the processing of personal data. In particular:

[35] Article 6 (4) GDPR.
[36] Article 6 (1) Data Act proposal.
[37] See also: vzbv (2022) Verbraucher:innen beim Data Act im Blick behalten: Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act).
[38] Article 6 (1) b) of the GDPR. This is confirmed by the European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p. 8 *et seq*.

- Article 1(3) of the Data Act should make clear that **if the processing of personal data made available to a data recipient pursuant to Article 5 is restricted in line with Article 6 of the Data Act, these provisions should be understood as taking precedence over Article 6 GDPR.**
- The Data Act should specifically state in a recital that, whenever personal data is concerned, the provisions of the Data Act should not undermine the protections of the GDPR but rather impose a stricter and more specific regime applicable to data generated by connected devices, to complement the rules of the GDPR. **The Data Act cannot establish new purposes for processing personal data on top of the GDPR regime**. It should only enable personal data to be used for **specific purposes**[39], such as aftermarket services or other narrowly defined "value added services" with consumers' consent[40].

➢ **Consumers should be able to meaningfully decide** what happens to data generated through the use of products and related services. This should be **applicable to all users** and not only those in highly concentrated markets like farming (as is currently indicated in Recital 25).

4.5. Mixed datasets

Out of necessity, the datasets covered by the Data Act will be mixed, containing personal and non-personal data, which in most cases may be inextricably linked (and in some cases may not even be easily and clearly distinguished, due to the GDPR's broad definition of personal data).[41]

The Data Act proposal offers no differential treatment to personal and non-personal data, relying on the GDPR to ensure protection of the latter.

Given that the Data Act does not seem to restrict sale of data by data holders, it is all the more crucial to reaffirm the protections to personal data under the GDPR.

BEUC recommendations

➢ The Data Act should **clarify what should be considered personal and non-personal data in line with the GDPR and the Data Governance Act** respectively.

➢ When personal and non-personal data in a dataset are inextricably linked, the data protection rights and obligations stemming from **the GDPR should fully apply to** the whole **mixed dataset**, thus attaining convergence with Article 2(2) of the Free Flow of Non-Personal Data Regulation.

4.6. Anonymisation

'Non-personal' data will often mean in practice 'anonymised' data. The quality of anonymisation may vary depending on the processes applied. High quality anonymisation is key to ensuring that non-personal data remains non-personal and cannot always be relied upon to prevent de-anonymisation.[42] This issue is not explicitly reflected in Recital

[39] In line with the EDPB-EDPS Joint Opinion 02/2022 on the Data Act, para. 55; and in Drexl, Banda et al. (2022) Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022, para. 16-19, 64.
[40] These purposes are both included in Recitals 14 and 28 and in the Impact Assessment (pp. 33, 34).
[41] See the argument in Drexl (2018) p. 5.
[42] AEPD-EDPS (2021) 10 misunderstandings relating to anonymisation. See also Drexl (2018) p. 5.

26 GDPR which only speaks of "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[43] It is also not addressed by the Data Act.

BEUC recommendation

- Given the possible risks of non-personal data processed and shared under the Act leading to somebody becoming personally identifiable, be it via cross-referencing with other data or other forms of de-anonymisation, the Data Act should include specific provisions to prevent such practices throughout the value chain. This should take the form of **specific requirements towards anonymisation or specific standards to ensure its robustness.**[44] This may possibly require the introduction of stronger protection concepts,[45] with requirements intended to make de-anonymisation impossible or at least considerably more difficult.

5. The Data Act as a way to foster competition

5.1. Protection for data holders: a risk of petrifying data monopolies

The Data Act proposal aims to reconcile two conflicting interests:

- to achieve more fairness in the allocation of value of data, including fostering the creation of new innovative products, supporting market choice and preventing vendor lock-in, by mandating data access rights to users which are meant to meaningfully control data; and
- to protect the innovation which already exists in the form of investments already made by data holders which should not be undermined.[46]

In respect of the latter goal, the Data Act should not tacitly assume that data holders enjoy a primary *erga omnes* right to all data generated by their products, from which the users' rights and the potential third-party rights merely constitute an exception.

Notably, the right of data holders over the data their devices generate is not an intellectual property (IP) right. Article 35 of the Data Act clearly excludes application of the Database Directive[47] to databases covered by the Act. This rules out the (potential) interpretation that the Data Act applies in parallel to the *sui generis* IP right to databases established in that Directive.

However, given the wording of the proposal, IP protection for the data holders may not be ultimately necessary. Through its technical framework, the Data Act proposal puts data holders in a position of **factual control** over data, leaving little space for the 'meaningful control' the Act promises to users:[48]

---

[43] Article 29 Data Protection Working Party published an opinion on anonymisation techniques, concluding that anonymisation may achieve the goal of creating a truly anonymous data set; however, it is a complex task that depends on the quality of the used techniques and their correct implementation on a case-by-case basis. See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[44] See also vzbv (2022) p. 16.
[45] For a more in-depth discussion, see vzbv (2022) p. 14.
[46] Recital 28.
[47] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (the 'Database Directive').
[48] Kerber W (2022) p. 6, 7, 15 *et seq*.

a) **On-site data access**. While 'access' itself is not defined, the proposal suggests that users and third parties will only access data either on the product itself, or on the cloud servers of the data holder. This puts the data holder in a position of considerable power, including enabling monitoring interactions of users and third parties with the data generated by the product.

b) **Monitoring of interactions with data**. As if to offset the necessity for users and third parties to access data within an environment controlled by the data holder, Articles 4(6) and 5(5) contain protection clauses that prohibit data holders to use data from their monitoring of such access and interactions to undermine the market position of, respectively, users and such third parties, in the markets in which they are active.

   However, this also means that:

   (i) such monitoring of users or third parties is generally allowed,

   (ii) data holders may use such surveillance for all purposes other than undermining the market position of the user or third party. In effect, the smaller the market reach of an entity, the more uses can be legitimised for its monitoring data;

   (iii) monitoring of the activities of users who are not businesses (e.g. consumers) is not curtailed in the current proposal.

c) **Data contracts**. Article 11 regulates contracts between data holders and third parties in a way that brings them close to licensing agreements with far-reaching protections for the data holder. Prevention of unauthorised access is addressed in the context of use for unauthorised purposes, abuse of gaps in the infrastructure, as well as unauthorised disclosure. A breach may require, at the option of the data holder, certain measures including:

   - mandatory destruction of the data along with any copies of this data;
   - mandatory destruction of any goods made based on this data, as well as
   - cessation of production, offering, placing on the market or use of such goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods.[49]

In short, users and third parties alike are forced into a situation where data holders benefit from *de facto* exclusivity:[50] they maintain technically exclusive control over the data which is accessible only through their infrastructure (products or servers). It has been pointed out that this *de facto* control is the economic equivalent to being granted legal exclusive IP-like rights on these data.[51]

BEUC recommendations

- The Data Act should not perpetuate the idea that device-generated data is 'owned' by manufacturers/data holders, which turns them into gatekeepers of the data generated by the products they sell. In particular:
  - the **measures in the event of a breach under Article 11** should be **limited to** situations where the unauthorised use or access took place in relation to data constituting a **trade secret**.

[49] Article 11 (2).
[50] Drexl J (2018) Data access and control in the era of connected devices, BEUC, Brussels.
[51] Kerber (2022) p. 15.

- The restrictions on **the monitoring** of users' interactions (including consumers) with third parties by data holders with data under Article 5(5) should not be limited to cases where there is a risk of undermining their actual market position. Instead, monitoring of such interaction should **only** be allowed **based on objectively justified security considerations.**

5.2. Restrictions for gatekeepers to access data

BEUC **welcomes** Article 5 (2) and Article 6 (2) (d) on restrictions to access data by gatekeepers designated under the Digital Markets Act (DMA). These provisions will be important to fight data concentration.

BEUC considers that this can be a way to stop gatekeepers from leveraging their market power into new markets, which was a similar policy goal in the DMA that we welcomed. At the same time, it is worth noting it does not prevent innovation by gatekeepers as Recital 36 says that gatekeepers can obtain this data through other lawful means. In other words, although the Data Act proposal excludes gatekeepers from new data rights, it does not stop gatekeepers from getting the data in other legal ways. For example, under Article 6 (9) of the DMA, end-users have the right to data portability so consumers can transfer their data from one gatekeeper to another service provider, including another gatekeeper, if they wanted to.

Finally, we generally support the principle of effective interoperability in Chapter 8 as an important element to deliver more competition and consumer choice.

6. Swift and effective redress and enforcement as preconditions for success

We welcome that competent authorities must cooperate with other Member State authorities (Article 31 (3) (f)). We also welcome that in respect to matters of data protection, the competent authorities will be those responsible for monitoring the application of the GDPR (Article 31 (2) a)). However, the practical arrangements between data protection authorities and those authorities in charge of the rest of the proposal are far from clear and can lead to inefficiencies in the future.

BEUC also welcomes that the Data Act proposal ensures a right to lodge a complaint (Article 32), but we regret that there is no procedural harmonisation and that the country of origin principle is followed to handle complaints. This has negative consequences notably for cross-border cases. As seen with other EU laws like the GDPR, this risks leading to forum and enforcement shopping.

Complaints are to be handled without undue delay and may result in application of 'dissuasive' financial penalties which are to be put in place at Member State level (Article 31 (3) d), Article 33). However, Article 33 does not harmonise the penalties that can be imposed. This could lead to forum and enforcement shopping by infringers of the Data Act.

On a more positive note, BEUC strongly welcomes that representative actions by consumers are possible thanks to the addition of the Data Act to the Representative Actions

Directive[52] Annex (Article 37). We also welcome that the Data Act is also included in the Annex of the Consumer Protection Cooperation Regulation[53] (Article 36).

BEUC recommendations

- BEUC welcomes **Data Protection Authorities** being **in charge of enforcing the Regulation in relation to personal data.** However, to ensure effective redress and enforcement, the proposal should include a **detailed cooperation mechanism** between DPAs and other competent authorities.
- BEUC recommends including **specific remedies** for consumers to seek redress if data holders or third parties do not respect their obligations.
- The enforcement mechanism needs to specify **further details** (e.g. deadlines, definition of handling a complaint, etc) not to repeat the same mistakes as with the cross-border enforcement of the GDPR.
- Article 33 should have a new paragraph establishing **minimum penalty amounts** (fines included) for infringements other than those set forth in Article 33 (3) and (4). This will lead to more harmonisation and prevent that it becomes cheaper to break the law in one Member State than another.
- BEUC welcomes and strongly supports the **inclusion** of the Data Act in the framework of the **Representative Actions Directive and the Consumer Protection Cooperation Regulation**.

- END –

[52] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC ('Representative Actions Directive').
[53] Regulation (EU) 2017/2394 on Cooperation between national authorities responsible for the enforcement of consumer protection laws ('Consumer Protection Cooperation Regulation').

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.