verbraucherzentrale
Bundesverband

RECOMMENDATIONS TO IMPROVE THE DATA ACT

Recommendations of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) on the Data Act trilogue negotiations

18. April 2023

Impressum

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.

Digitales und Medien
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister registriert. Sie erreichen den entsprechenden Eintrag hier.

INHALT

I. CORE RECOMMENDATIONS

- vzbv calls on the Council and Parliament to reconsider their positions and exclude highly sensitive devices, such as smartphones, from the scope of the Data Act.
- It should be clarified in Article 1 (3), that the Data Act does not create a legal basis for the processing of personal data and that in case of conflict of interpretation between the Data Act and the European data protection law, the latter prevails. The Council should agree to the respective proposals of the Parliament.
- The Parliament clarifies in Article 1 (4a) that the Data Act complements the Unfair Commercial Practices Directive, the Consumer Rights Directive and the Unfair Contract Terms Directive and does not affect their applicability. vzbv welcomes this and calls on the Council to agree.
- The Parliament should follow the Council in making it clearer, that where the user is not the data subject, the Data Act does not create a legal obligation to provide access to personal data or make it available to a third party and should not be understood as conferring any new right on the data holder to use data.
- The Council should support Article 3 (1) of the Parliament's position, that connected products shall be designed and manufactured in such a way that a data subject can use the products in the least privacy-invasive way possible.
- The Council's position provides in Article 4 (1a) that any agreement between the data holder and the user shall not be binding when it narrows the users' access rights. Also, according to Article 7 (3), any contractual term which excludes the application of or derogates from the user's rights shall not be binding on the user. Here, the Parliament should follow the position of the Council.
- vzbv welcomes that both the Council and the Parliament want to prevent the use of deceptive designs by data holders and data recipients. However, the wording of the provisions should be aligned with the corresponding wording of Article 13 (6) Digital Markets Act, as proposed by the Parliament in Article 4 (1) (d) and Article 6 (2) (a).
- Users should be truly free to decide how their data may be used. Therefore, data holders should not be allowed to make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service, as proposed by the Parliament in Article 4 (6). The Council should support this amendment.
- To allow users to benefit from a fair market for non-personal data, data holders should only be permitted to use non-personal data accessed by users' connected products to improve the functioning of the connected product or to develop new products. They should be allowed to provide the data to third parties in aggregated form or to fulfil of their contractual obligations to the user. The Parliament has made good proposals in Article 4 (6a) and (6b), which the Council should endorse.
- The Council should adopt the Parliament's position, expressed in Article 5 (1), that personal data shall be only processed by data recipients for purposes specified by the data subject. On the other hand, the Parliament should agree with the Council's Article 6 (1) (b) that a data recipient shall not use the data it receives for the profiling of natural persons, unless it is objectively necessary for a purpose that is integral to the delivery of the service requested by the user.

II. BACKGROUND

In February 2022, the European Commission (Commission) published the proposal for the Data Act.[1] It aims to promote the availability of data while respecting fundamental European values. The Data Act is intended to regulate the conditions under which companies or consumers can obtain data generated by their connected devices and make it available to other parties. In March 2023, both the European Parliament[2] (Parliament) and the Council of the European Union[3] (Council) agreed on their respective positions and entered the informal trilogue negotiations.

The following remarks and recommendations by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) refer primarily to the provisions on data sharing between businesses and users. Although both institutions have improved the Commission's draft in this regard, it is still questionable whether the Data Act is actually suitable for achieving its intended goals. Under no circumstances should the Data Act lower the existing level of consumer and data protection.

III.CRITICAL REMARKS

Based on the positions of the Council and the Parliament, it is still questionable whether the goals envisaged by the Data Act can be achieved. The provisions are still very complex, especially in relation to other European and national legislation, but due to the horizontal orientation of the Data Act they are nevertheless quite general, making them difficult to apply in practice. Many purposes (such as optimised training of algorithms) will continue to be unachievable because of the user-centric nature of the Data Act. In addition, the Council and Parliament grant data holders further options for preventing access to data, for example by referring to their trade secrets.

It is also problematic that the Data Act tries to treat very different situations in the same way. It is regrettable, for example, that none of the institutions introduced a better distinction between B2B and B2C situations, as demanded not only by consumer associations but also by various business stakeholders. A clearer separation of the spheres and the associated requirements could have led to a higher level of protection for consumers and, at the same time, to greater freedom and more legal certainty for business.

---

[1] Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A0068%3AFIN

[2] Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). T9-0069/2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.html

[3] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) - Mandate for negotiations with the European Parliament. ST 7413/23 INIT. https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf

Also, none of the proposals sufficiently differentiates between personal and non-personal data, for the processing of which the European law provides different requirements. Most provisions refer to both categories of data, which makes the distinction very difficult and leads to ambiguities in interpretation. Here too, a clearer separation of the data categories and the associated requirements could have led to more legal certainty and reduced risks for data subjects.[4] In any case, mixed data sets should still always be classified as personal data.

It is particularly critical that, although the Data Act creates new risks for data subjects by, for example, enabling continuous and real-time access to personal data, it does not take sufficient account of these new risks. If the legislator creates new possibilities for processing personal data via legal acts, he must at the same time introduce new measures to protect the rights of the data subjects, so that the balance is not shifted even further to their disadvantage. For example, it would have been appropriate to limit the purposes for which data recipients may process the personal data they receive through the new possibilities of the Data Act.

Another serious factor is that, according to the proposals of the Council and the Parliament, data generated or collected by smartphones will be included by the Data Act[5] – contrary to the recommendations of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).[6] Smartphones can be assigned to a specific person in almost all cases and are used for confidential communication. At the same time, a large number of sensors are installed in these devices that generate – supposedly non-personal – data. Yet, this data can provide detailed information about the user's life situation and communications. U.S. researchers have recently shown, for example, that it is possible to draw conclusions about the caller and the content of a conversation by accessing the data generated by a smartphone's motion sensors. [7]

This example shows that accessing data stored on a smartphone poses major risks and that it is very difficult to anticipate and assess these risks. Facilitating access to this data, as it would be the case if smartphones were included in the scope of the Data Act, would further increase already existing risks to the protection of personal data, privacy and confidential communication. However, it would fall short to shift this risk assessment to the consumers.

VZBV RECOMMENDS

vzbv calls on the Council and Parliament to reconsider their positions and decide to exclude highly sensitive devices, such as smartphones, from the scope of the Data Act due to the unmanageable risks to the protection of personal data, privacy and confidential communication.

---

[4] See European Data Protection Board; European Data Protection Supervisor: 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), 2022, paragraph 27. https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf, 12.04.2023.

[5] The Council and Parliament deleted the passages in Recital 15 that explicitly excluded devices such as smartphones from the scope of the Data Act.

[6] See footnote 4, paragraph 42

[7] Toulas, Bill: EarSpy attack eavesdrops on Android phones via motion sensors, 2022, https://www.bleepingcomputer.com/news/security/earspy-attack-eavesdrops-on-android-phones-via-motion-sensors/, 12.04.2023.

IV. RELATIONSHIP TO THE EUROPEAN DATA PROTECTION LAW

The Commission's proposal does provide in Article 1 (3) that the application of European law on the protection of personal data, privacy and confidentiality of communications remain unaffected. However, this intended demarcation of the Data Act from data protection law is not always sufficient.[8] vzbv therefore welcomes that both, the Parliament and the Council, are seeking to define this demarcation better.

For example, the Council makes clear in Recital 5, that any processing of personal data should comply with all conditions and rules provided by data protection legislation, including the need for a valid legal basis under the General Data Protection Regulation (GDPR) and the ePrivacy-Directive. In particular, the Council clarifies in Recital 24 that where the user is not the data subject, the Data Act does not create a legal basis to provide access to personal data or make it available to a third party and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. However, these remarks in the recitals were not included in the articles of the Council position, which should be corrected in the trilogue negotiations.

In addition, vzbv still believes that there is need for a rule, stipulating that in case of conflicting provisions, European data protection and privacy legislation should prevail over the Data Act – as proposed by the Parliament in Article 1 (3). This amendment is in line with the wording of Article 1 (3) of the Data Governance Act and with the EDPB-EDPS Joint Opinion 02/2022[9].

Furthermore, the Parliament has made a very important proposal in Article 3 (1), that connected products shall be designed and manufactured in such a way that a data subject can use the products in the least privacy-invasive way possible. This amendment – also proposed by the EDPB and EDPS[10] – is important because while processors of personal data are covered by the GDPR, mere manufacturers of products are not.

As explained above, the Data Act creates new possibilities for the processing of personal data without simultaneously introducing new measures to adequately protect the rights of data subjects in order to maintain the existing balance. In particular, it is problematic that the Data Act does not limit the purposes for which data recipients may process personal data. The Parliament at least tries to mitigate the risks by emphasising in Article 5 (1) that personal data may only be processed by data recipients for purposes specified by the data subject, such as the provision of after-market services. Although this is not sufficient in vzbv's view, the Council should adopt this position of the Parliament.

On the other hand, in Article 6 (1) (b) the Council seeks to minimise some of the risks by providing the position that a data recipient shall not use personal data it receives

---

[8] See Verbraucherzentrale Bundesverband: Verbraucher:innen beim Data Act im Blick behalten, 2022, page 6ff. https://www.vzbv.de/sites/default/files/2022-05/22-05-13_vzbv-Stellungnahme_Data-Act.pdf, 12.04.2023.

[9] See footnote 4, paragraph 26

[10] See footnote 4, paragraph 47

pursuant to the Data Act for the profiling of natural persons, unless it is objectively necessary for a purpose that is integral to the delivery of the service requested by the user. The Parliament just emphasises that profiling has to be conducted in compliance with the GDPR, which should be a matter of course in vzbv's opinion. To better protect users, the Parliament should agree with the Council's position.

VZBV RECOMMENDS

It should be clarified in Article 1 (3) of the Data Act, that it does not create a legal basis for the processing of personal data and that in case of conflict between the Data Act and the European data protection law, the latter prevails. The Council should agree to the respective proposals of the Parliament.

The Parliament should follow the Council in making it clearer, that where the user is not the data subject, the Data Act does not create a legal obligation to provide access to personal data or make it available to a third party and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service.

The Council should support Article 3 (1) of the Parliament's position, that connected products shall be designed and manufactured in such a way that a data subject can use the products in the least privacy-invasive way possible.

In order to at least somewhat offset the new risks that the Data Act creates for consumers, the Council should adopt the Parliament's position, expressed in Article 5 (1), that personal data shall be only processed by data recipients for purposes specified by the data subject, such as the provision of after-market services. On the other hand, the Parliament should agree with the Council's Article 6 (1) (b) that a data recipient shall not use the data it receives for the profiling of natural persons, unless it is objectively necessary for a purpose that is integral to the delivery of the service requested by the user.

V. NEED FOR STRONG CONSUMER RIGHTS

The EU Commission is pursuing a number of goals with the Data Act. By making it easier for consumers and companies to access and use data, it is intended to ensure that the value created from data is distributed fairly among the players in the data economy. One fear expressed by economists in the debate, however, is that the Data Act as proposed by the commission will not dissolve the previous de facto power of data holders to dispose of the data generated, but that it will rather strengthen and legally cement their position.[11]

This is because one of the core elements of the Commission's proposal is that contracts for data use be concluded between the various parties. In addition to the actual purchase contracts, consumers will therefore in the future also have to decide on the

[11] See for example Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives, 2022, https://ssrn.com/abstract=4080436, 12.04.2023.

purpose and scope of the use of their data. Especially in B2C situations, data holders could exploit existing power imbalances and secure rights to non-personal data quite easily through such contractual agreements with users. For most consumers, it will be nearly impossible to assess the implications of their choices. Moreover, they will have no way to influence the form and content of contracts. So, consumers need effective protection against unfair and harmful practices by companies. The Commission's approach of referring to existing consumer protection law in the recitals alone and mandating pre-contractual information is not sufficient.

For these reasons, vzbv welcomes that the Parliament clarifies in Article 1 (4a) that the Data Act complements the Unfair Commercial Practices Directive, the Consumer Rights Directive and the Unfair Contract Terms Directive and does not affect their applicability. vzbv calls on the Council to agree to this amendment.

On the other hand the Council's position declares in Article 4 (1a) clauses between the data holder and the user as non-binding if they restrict the users' access rights. Also, according to Article 7 (3) of the Council's position, any contractual term which excludes the application of or derogates from the user's rights shall not be binding on the user. Here, the Parliament should follow the position of the Council to prevent that consumers unwittingly agree to contractual terms to their disadvantage.

It is also important that users are actually free to decide how their data may be used. In particular, situations should be prevented in which users have to make a take-it-or-leave-it decision. Such decision-making structures not only restrict users' freedom of choice, they also favour companies with great market power and help them to further expand their position. Therefore, data holders should not be allowed to make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service, like proposed by the Parliament in Article 4 (6).

Also, vzbv welcomes that both the Council and the Parliament want to prevent the use of deceptive designs ("dark patterns") by data holders and data recipients. However, the wording of the provisions should be aligned with the corresponding wording of Article 13 (6) Digital Markets Act, as proposed by the Parliament in Article 4 (1) (d) and Article 6 (2) (a). Merely prohibiting data recipients to "coerce, deceive or manipulate the user, by subverting or impairing the autonomy, decision-making or choices of the user" would not adequately protect consumers. According to this wording, intent would have to be proven in order to take action against such deceptive designs, which is hardly feasible in practice.

In addition, users should also benefit from a fair market for non-personal data, as is the Commission's goal. To enable users to create value in the data markets, they should have the exclusive right to sell the non-personal data generated by their individual products, as proposed by the Parliament. Data holders on the other side should be permitted to use non-personal data accessed from users' connected products to improve the functioning of the connected product or to develop new products. In addition, they should be allowed to provide the data to third parties in aggregated form or to fulfil their contractual obligations to the user. The Parliament has made good proposals in this regard in Article 4 (6a) and (6b), which the Council should endorse.

VZBV RECOMMENDS

The Parliament clarifies in Article 1 (4a) that the Data Act complements the Unfair Commercial Practices Directive, the Consumer Rights Directive and the Unfair Contract Terms Directive and does not affect their applicability. vzbv welcomes this and calls on the Council to agree.

The Council's position provides in Article 4 (1a) that any agreement between the data holder and the user shall not be binding when it narrows the users' access rights. Also, according to Article 7 (3), any contractual term which excludes the application of or derogates from the user's rights shall not be binding on the user. Here, the Parliament should follow the position of the Council.

Users should be truly free to decide how their data may be used. Therefore, data holders should not be allowed to make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service, like proposed by the Parliament in Article 4 (6). The Council should support this amendment.

vzbv welcomes that both the Council and the Parliament want to prevent the use of deceptive designs ("dark patterns") by data holders and data recipients. However, the wording of the provisions should be aligned with the corresponding wording of Article 13 (6) Digital Markets Act, as proposed by the Parliament in Article 4 (1) (d) and Article 6 (2) (a).

To allow users to benefit from a fair market for non-personal data, data holders should only be permitted to use non-personal data accessed from users' connected products to improve the functioning of the connected product or to develop new products. In addition, they should be allowed to provide the data to third parties in aggregated form or to fulfil of their contractual obligations to the user. The Parliament has made good proposals in this regard in Article 4 (6a) and (6b), which the Council should endorse.