The Consumer Voice in Europe

DATA GOVERNANCE ACT

BEUC position paper

Contact: 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-2021-026 - 29/03/2021

Why it matters to consumers

Consumers generate more and more data every day. The sharing and reuse of such data can benefit consumers and society as a whole. For example, data can power the development of new and innovative services and help improve urban mobility to reduce emissions and combat climate change. However, consumers often cannot control how the data that they generate is used. The EU's approach to data governance – as proposed by its Data Governance Act – must ensure the protection of fundamental rights, and foster competition, consumer choice and innovation that benefits consumers. This is key for achieving a fair, healthy and sustainable digital economy.

Summary

This paper provides BEUC's views on the Commission's proposal[1] for a 'Data Governance Act' (DGA). The DGA will create an umbrella law through which data – and that, of course, includes consumer data – can be legally shared in particular sectors. Think of data-sharing between research institutes and patients, for instance. Or mobility data sharing to tackle climate change This horizontal law should then be followed up with specific sectoral legislative and non-legislative tools with guidance on how data-sharing plays out in health or mobility.

BEUC welcomes that, in line with the European Data Strategy, the DGA is striving to create a human-centric approach for the digital single market and the data economy. In particular, we welcome the intention to foster data sharing mechanisms that benefit society as a whole, by allowing the re-use of public sector data and the sharing of such data for the common good. BEUC appreciates the Commission's efforts in seeking to create a trustworthy and rules-based data sharing ecosystem. We welcome that such ecosystem is designed to be transparent when it comes to the actors involved.

However, the success of the DGA depends on its interplay with other EU legislation including the General Data Protection Regulation (GDPR), Open Data Directive the ePrivacy Directive, as well as with any future legislation regulating the sharing of personal information such as the upcoming Data Act. In the DGA proposal this interplay is not always clear and raises significant concerns. Although the DGA is not meant to interfere with or modify existing data protection rules, it would be important to clarify that it does not operate in a vacuum and where it provides for exception (or lex specialis) to the General Data Protection Regulation (GDPR), there should be no conflict with the principles governing the collection and processing of personal data.

In this context, we highlight the following points:

- It is crucial **to clarify the interplay between the DGA and the GDPR**. These two important pieces of law must not conflict. More specifically, the DGA should make clear that, insofar as personal data processing operations are concerned, the GDPR takes precedence over the DGA. The DGA must not undermine the protection of personal data provided by the GDPR.

[1] Proposal for a Regulation on European data governance (Data Governance Act) -COM (2020) - 767 final2020/0340 (COD).

- The **provisions regarding the re-use of data held by public authorities should only apply to non-personal data**. Personal data should not fall in the scope of Chapter II of the Regulation. Consequently, personal data should not be included in the list of 'protected data' in this Chapter.
- A **clear definition of what would constitute 'purposes of general interest'** should be introduced, given the importance of this concept and the different interpretation that might exist at national level.
- **'Data intermediaries' should be clearly defined and should be subject to stricter rules**. Some of the provisions which are now in the Recitals should be integrated in the Articles of the Regulation. For example, Recital 22, which states that intermediaries should not act as 'data brokers' in the context of digital advertising.
- **Legislators should avoid introducing new concepts such as 'data altruism'** which are likely to overlap with the concepts included in the GDPR. Sharing of personal data is regulated by the GDPR so there is no need to create competing regimes. Thus, BEUC does not see the need to regulate such sharing in the context of the DGA.
- **Data Protection Authorities should be responsible** for the interpretation and enforcement of the DGA provisions regarding the processing of personal data.

1. The objectives of the Data Governance Act and the relationship with the GDPR

1.1. Fostering the availability, sharing and use of data for the common good

The proposed Data Governance Act[2] (DGA) is striving to create a trustworthy, rule-based and human-centric approach for the digital single market and the data economy, by fostering data sharing mechanisms that benefit society as a whole and by allowing the re-use of public sector data and the sharing of such data for the common good.

1.2. The protection of personal data and the relationship with the GDPR

The DGA aims at facilitating the exchange and use of personal and non-personal data. First and foremost, there should be a clearer distinction between these two categories of data in the proposal and the obligations applying for each. As it stands, the proposed regulation does not clearly separate the two categories of data and the associated requirements. This may lead to legal uncertainty. In this context, we have to underline that the protection of personal data is already subject to specific rules, namely the General Data Protection Regulation (GDPR)[3]. The DGA proposal does not necessarily provide the same level of protection as the GDPR.

Therefore, **our main concern is that the DGA may weaken the protections ensured by the GDPR by creating an exception (or *lex specialis*) which private entities and public institutions can use to bypass the application of the existing rules.** For this reason, before proceeding with further analysis of the DGA proposal, it is key to recall that, insofar as personal data is concerned, the use of such data must take place in full respect of the GDPR. It should also be underlined that, since datasets can combine personal and non-personal data, access to mixed data sets that contain both types of data should be governed by the rules of the GDPR[4].

[2] Proposal for a Regulation on European data governance (Data Governance Act) -COM (2020) - 767 final2020/0340 (COD).
[3] Regulation (EU) 2016/679.
[4] See the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM(2019) 250 final).

It is particularly worrisome that the combination of the provisions of Chapter II on the re-use of 'protected data' and of Chapter III on 'data intermediaries' opens the possibility to allow the data intermediaries to define the purposes of data sharing. The focus should be on ensuring that consumers are in full control of what happens with their personal data. This will be achieved only by stimulating the developments of technical solutions to allow consumers to control with whom they share data as well as through the consistent enforcement of the GDPR and the consumer protection legislation (e.g. against misleading and manipulative practices in interface design (choice architecture)). The provisions regarding 'data altruism' in Chapter IV of the proposal also raise some concerns from this perspective, as explained further below.

If consumers were to provide access to their data for research under a public purpose research initiative, this should not be for commercial purposes. Should the outcome of the research then contribute to the development of a product or service that is exploited commercially, conditionalities should apply to the use of this research derived from the data supplied by consumers. A research outcome such as a new medicine should then not be licensed on exclusive basis and allow further access and use of research results.

Furthermore, if a product or service is developed as a result of using such consumer data, this must be reflected in its price: That is, it should be accessible and affordable for all. Consumers must also be legally protected against misleading practices which are presented as public purpose research when in reality there is commercial intent in the exploitation of the data as a result of the commercialisation of the research outputs.

Considering the above, the DGA must make clear that personal data protection is subject to the GDPR. For example**, it should be explicitly stated in Art.1 of the proposal that the DGA, in its entirety, is without prejudice to the provisions of the GDPR**.

2. Re-use of 'protected data' (Chapter II)

2.1. Personal data should be excluded from the scope of the public sector data re-use regime (Art 3)

Chapter II of the DGA seeks to create a mechanism for re-using certain categories of 'protected public sector data'[5], including personal data. As highlighted in the previous section, we underline that when personal data is processed, the GDPR should be the only applicable law.

Moreover, in this specific context of the re-use of public data, we do not see any added value to include personal data processing activities in the scope of the DGA. The re-use of personal data is already possible under the GDPR and it should be governed only by its provisions.

What is more, under the GDPR, the purpose limitation principle protects data subjects by setting limits on how data controllers are able to use their data (Art 5 (1)(b)). Such principle has two main building blocks: personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use). Further processing for different purposes is possible, provided that the data subject gave their specific consent or that the new purpose is compatible with the original purpose. In this second case, a substantive compatibility assessment on a case-by-case basis has to be carried out. Such assessment

[5] Protected data are defined by art 3 as 'data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality; (b) statistical confidentiality; (c) protection of intellectual property rights of third parties; (d) protection of personal data.

requires an evaluation of all relevant circumstances (the relationship between the purposes for which the personal data have been collected and the purposes of further processing; the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use; the nature of the personal data and the impact of the further processing on the data subjects; the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects)[6].

It becomes evident that the further processing (re-use) of personal data is already possible under the current rules. We regret that by allowing third parties to re-use consumers' personal data without clearly providing with the same safeguards described above, the DGA risks creating legal uncertainty and undermining the protection granted by the GDPR.

In addition, pursuant to art. 6, public sector bodies which allow re-use of 'protected data' may charge fees for allowing the re-use of such data. If this includes personal data, there is a risk of incentivising public bodies to "commercialise" consumers' personal data. Although BEUC appreciates that any fees shall be non-discriminatory, proportionate, objectively justified and shall not restrict competition, it is important to prevent any unintended consequences or adverse effects on the protection of fundamental rights.

We therefore ask for **personal data not to fall in the scope of Chapter II.** Consequently, personal data should be deleted from the list of 'protected data' in art. 3. The provisions regarding the re-use of public sector data should only cover non-personal data.

2.2. Prohibition of exclusive agreements (art. 4)

The Commission rightly prohibits agreements or other practices pertaining to the re-use of 'protected data' held by public sector bodies that would grant exclusive rights or restrict the availability of data for re-use by entities other than the parties to such agreements. At the same time, by way of derogation from such provision, the DGA envisages that an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or a product 'in the general interest'.

Although BEUC understands the rationale for such a derogation, the concept of 'general interest' is vague (please see also below section 3 on 'data altruism') and remains undefined. This could create an exception that is too broad and general. We therefore invite the legislators to refine this exception and namely **to further describe the concept of 'general interest'**, for example by adding in Article 2 a definition with a list of criteria to be met in order for a service or a product to be considered to be "in the general interest" and be able to make use of this exception.

2.3. Conditions for re-use (art. 5)

BEUC welcomes that public sector bodies shall make publicly available the conditions for allowing the re-use of 'protected data' and that such conditions should be non-discriminatory, proportionate, and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed. Equally, BEUC welcomes that such conditions shall not be used to restrict competition.

However, we highlight the need to **delete the reference to pseudonymisation in paragraph (3) of art. 4**. The provision *de facto* equalises anonymisation and pseudonymisation, which are two different concepts with different consequences in terms of data protection. The re-identification of the data subject cannot be excluded when data

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 03/2013 on Purpose limitation: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

is pseudonymised, while in principle it should not be possible if personal data is duly anonymised.

Regarding paragraph (6), it is unclear how 'the public sector body shall support re-users in seeking consent of the data subjects. This aspect should be clarified. In particular, such 'support' must not turn into nudging data subjects to consent without properly understanding the consequences connected to the re-use of their personal data.

Finally, we underline the need to ensure redress for consumers. In this sense, it is key that consumer organisations can seek remedy, enforce a high level of protection and represent the collective interest of consumers in case of infringements of the DGA. We stress the need to expand article 8 of the DGA accordingly and include the DGA in the list of Union law of Annex I of the Representative Actions Directive[7].

3. Data sharing providers ('data intermediaries') – Chapter III

The proposal aims to increase trust in sharing personal and non-personal data and to lower transaction costs linked to B2B and C2B data sharing by creating a notification regime for 'providers of data sharing services' (data intermediaries). More specifically, the Commission intends to create a network of trusted and neutral data intermediaries that collect and process data. This would cover, among other, intermediation services between data subjects that seek to make their personal data available and potential data users.

Data intermediaries will have to notify the competent authority designated by the Member States that they intend to provide intermediation services and will have to comply with a number of requirements, including the obligation not to use the data for other purposes than those notified to the authority. The competent national authority will also be responsible for monitoring compliance with the legal requirements.

BEUC welcomes the overall aim to further regulate data intermediaries in the context of the DGA, but certain elements should be improved.

A precise definition of what is a 'data intermediary' should be introduced in art. 2 of the proposal.

At the moment the only references to this point come in the recitals. According to recital 22, this concept of 'data intermediaries' should only cover services aiming at 'intermediating between an indefinite number of data holders[8] and data users[9], excluding data sharing services that are meant to be used by a closed group of data holders and users. The recital further clarifies that 'providers of cloud services' as well as 'advertisement or data brokers, data consultancies, providers of data products resulting from value added to the data by the service provider' should not be able to act as data intermediaries. Equally, recital 23 clarifies that the business models of intermediaries must ensure that there are no misaligned incentives that encourage individuals to make more data available for processing than what is in the individuals' own interest.

[7] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0184

[8] According to art. 2(5) 'data holder' means a legal person or data subject 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.

[9] According to art. 2(6) 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes.

Those exclusions and clarifications should also be reflected in the definition to be added in the text. This aspect is crucial. At the moment, data intermediation often happens in the context of the ad-tech industry. Research by BEUC members, such as Norway's Forbrukerrådet, has highlighted serious concerns about the compliance of these actors with privacy, data protection and consumer laws[10]. Such actors use information to constantly track consumers in order to create comprehensive profiles about them. In turn, profiling is used to personalise and target advertising, and it can lead to discrimination, manipulation and exploitation of consumers. It is of utmost importance to that ad-tech actors will not be able to act as 'data intermediaries' in the sense of the DGA.

We welcome that under the Act, data intermediaries will have to comply with precise and strict requirements such as: notifying the relevant member State authority of their intent to provide intermediation services; appointing a legal representative in the EU, if the provider is not established in the Union; or acting in the data subject's best interest when facilitating the exercise of data subjects' rights.

However, several questions arise when it comes to the transmission of personal data through these providers. Regardless of the obligation to respect the abovementioned requirements, the intermediation services between data holders and data users (which include the creation of platforms or databases) should only enable the exchange of data or facilitate the establishment of a specific infrastructure for the interconnection of data holders and data users. Article 9(a) currently refers to the 'joint exploitation' of such data.[11]. BEUC would like to stress that any operations involving personal data in the scope of Article 9 is subject to the rules of the GDPR and therefore the conditions for the joint use of the data is subject to these rules. Thus, instead of the term 'exploitation', we would suggest using the term 'use' as it is more compatible with the language of the GDPR.

Before promoting the development of personal data exchanges through data intermediaries, it is crucial to ensure that the rules governing the protection of personal data are efficiently enforced. Having a strong and coherent enforcement of such rules is an indispensable prerequisite to ensure a higher level of trust. The DGA must not result in greater flows of data passing through actors that are not diligent and seek to exploit personal data in their own interest or even against the interest of the data subjects.

3.1. The role of consumer organisations

Data intermediaries can have an important role in seeking to enhance individual agency and the individuals' control over their data. For example, as also stated in recital 23, they would assist individuals in exercising their rights under the GDPR. In particular, they might help data subjects in managing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, etc.

We also stress the importance of compensating consumers in case their rights are infringed. In this context, consumer organisations can have an important role to play to restore trust towards data controllers by helping consumers to navigate the data economy. They can advise and guide consumers in their choices in an independent and trustworthy manner, for example by checking the legality of the practices of corporate actors and helping consumers take action if their rights are not respected. This is why, we think that consumer organisations may decide to act as data intermediaries themselves.

[10] See the report 'Out of Control' by the Norwegian Consumer Council https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/

[11] Art.9: '*The provision of the following data sharing services shall be subject to a notification procedure:* a) *intermediation services between data holders which are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or* ***joint exploitation of data,*** *as well as the establishment of a specific infrastructure for the interconnection of data holders and data users;(…)'*

4. Data altruism (Chapter IV)

Chapter IV of the DGA seeks to facilitate that individuals and companies make their personal and non-personal data voluntarily available for the common good ('data altruism'). To this end, the Act also establishes the possibility for organisations engaging in data altruism to register as a 'Data Altruism Organisation recognised in the EU' in order to increase trust in their operations. In addition, a common European data altruism consent form will be developed to lower the costs of collecting consent and to facilitate portability of the data (where the data to be made available is not held by the individual).

4.1. Overlap with the GDPR

By introducing the concept of 'data altruism', the DGA further regulates an activity (the processing of personal data for 'altruistic' purposes) that can already perfectly take place within the context of the GDPR. As previously stressed, if and when personal data processing activities take place, the GDPR is the applicable law. Therefore, we believe it is better to apply the provisions regarding data altruism only to the sharing of non-personal data only as the sharing of personal data based on the consent of a data subject for 'altruistic' purposes can already take place in respect of the GDPR.

The DGA itself underlines in the part relating to the 'European data altruism consent form' that *'Where personal data are provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a specific data processing operation in compliance with the requirements (of the GDPR)'* (art. 22(3)). We therefore question need for additional rules on personal data altruism, which, in turn, could create legal uncertainty and undermine the protection granted by the GDPR. In this sense, it would be preferable to limit the scope of the provisions related to data altruism to non-personal data.

4.2. 'Altruism' is a problematic label

The DGA defines 'data altruism' as '*the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services'* (art. 2). Although BEUC appreciates that such definition makes clear that the data subject's consent is needed for allowing the 'altruistic' sharing of data, we have concerns regarding the concept of 'altruism' itself and how it is defined in the proposal.

First, 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 personal data available for general interest purposes is unregulated, while this is covered by the GDPR. This is further illustrated by the fact that the definition of the concept in the DGA is linked to the concept of 'consent', which is a legal basis under the GDPR.

As already highlighted in our position paper on the EC's Data Strategy[12], 'data altruism' is a problematic term which can be misused to unduly influence consumers. The 'altruistic' element might be used to nudge consumers into a choice and behaviour which may not be justified depending on the circumstances. It might also entail problematic consequences for those consumers who are not willing to share their data. Further to this, labels such as "altruism" or "data donation" can be used to trick consumers into sharing personal data without them being aware of the potential commercialisation of these data by third parties afterwards. data. Should those consumers be seen as non-altruist human beings?

[12] https://www.beuc.eu/publications/beuc-x-2020-046_a_european_strategy_for_data_-_beucs_response_to_public_consultation.pdf

Furthermore, it is unclear what 'general interest' means in this context, as there is no precise definition in the Act. Services of general interest constitute a very broad concept in EU law. Such services can be of general economic interest (basic services that are carried out in return for payment, such as postal services); non-economic services, such as the police, justice and statutory social security schemes; or social services of general interest like those that respond to the needs of vulnerable citizens and are based on the principles of solidarity and equal access[13]. Allowing the sharing of personal data for generic 'public interest' purposes may endanger the respect of the fundamental right to personal data protection. It might also mislead consumers, as there are no clear legal benchmarks to check against the presence of such a 'general interest' ('altruism washing') and, in some cases, the interpretation of what constitutes a 'general interest' might differ at national level.

The only reference to purposes of 'general interest' in the Act can be found in recital 35 which includes '*healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services'*. In addition, the Act turns to Member States for further specifications under national law. In our view, what is to be considered a purpose of 'general interest' should be further specified in the DGA itself. A more precise definition with indicative criteria to assess what constitutes such a general interest, should be added under article 2 of the Act.

5. Competent authorities

BEUC appreciates the efforts of the Commission to create a strong enforcement ecosystem to ensure that the provisions of the DGA are fully respected. We underline the need to sufficiently equip the competent supervisory authorities both in terms of human and economic resources.

The DGA gives Member States the freedom to designate one or more competent authorities for monitoring the compliance with the rules regarding 'data intermediaries' and 'data altruism'. In this sense, we underline that, when personal data is processed, the Data Protection Authorities (DPAs) are the competent bodies for monitoring compliance in application of the GDPR. These authorities should also be competent for monitoring compliance with the DGA when there is processing of personal data.

In any event, we welcome that, in the context of data altruism, the Commission highlights that the designated authorities shall first seek an opinion or decision by the national DPA for any question requiring an assessment of compliance with the GDPR (art. 20(3)). Unfortunately, this is not envisaged in the context of data intermediaries. We therefore call on the legislators to also reflect this point in art. 12.

We also take this chance to highlight the need to have strong cooperation between different authorities (consumer protection, data protection, competition, etc), especially in a context such as the one laid down in the DGA where there may be an overlap between different competences.

END-

[13] https://ec.europa.eu/info/topics/single-market/services-general-interest_en

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