BEUC The European Consumer Organisation

The Consumer Voice in Europe

MY PERSONAL DATA, NOBODY'S BUSINESS BUT MY OWN

Key consumer demands for the trilogue on the General Data Protection Regulation

Contact: David Martin – 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 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2015-085 - 11/09/2015

Summary

BEUC reiterates the urgent need to put consumers back in control over the way their personal data is processed online and hopes an agreement on the General Data Protection Regulation will be reached under the Luxembourg Presidency.

However, the urgency to adopt the Regulation must not take its toll on consumers' fundamental rights. Weak provisions on fundamental data protection principles (e.g. purpose limitation) and/or allowing too much flexibility for commercial entities to process personal data based on their alleged legitimate interests could have devastating effects for consumers' privacy, especially if coupled with flawed rules on highly sensitive aspects like profiling.

In general terms, we believe that the European Parliament's first reading position provides a good basis for an agreement. We also welcome the proactive stance taken by the European Data Protection Supervisor, who has provided some useful recommendations. In contrast, the Council's General Approach contains some provisions that would even weaken current protection standards, a clear red line set out in the beginning of this reform.

That being said, we urge the Commission, the Parliament and the Council to be ambitious. The objective is to modernise and improve Europe's data protection regime, not to merely maintain the *status quo and certainly not to weaken existing protection.* The outcome of these negotiations shall provide consumers with greater transparency and control over how their personal data is collected and used. Otherwise consumers will be left with little option than to systematically give up their privacy in order to access online goods and services. This would be unacceptable.

A robust Data Protection Regulation must comprise:

A broad and future-proof scope. Every company doing business in Europe or targeting users based in Europe must comply with EU laws, regardless of the company's nationality or the place where it is established. Any kind of information that would allow to identify an individual or single someone out as an individual shall be considered personal data, including pseudonymous[1] data.

Solid data protection principles and strict legal grounds for data processing. Principles such as "purpose limitation" and "data minimisation" are at the core of the EU data protection regime and must not be weakened. The amount of personal data processed should be kept to the minimum necessary. Further processing of personal data for purposes incompatible with those that justified the initial processing should not be allowed.

An enhanced set of data subjects' rights. Strong and clear provisions are needed with regard to fundamental issues such as the information that must be provided to data subjects, profiling and the right to object. Restrictions on user rights should be strictly limited and include sufficient guarantees.

A comprehensive enforcement scheme, including effective mechanisms for consumer redress. The Regulation must be effectively and uniformly enforced across all of the EU. It is crucial that consumers can easily access effective mechanisms to seek redress and that consumer organisations are allowed to proactively defend the rights of data subjects.

[1] Pseudonymization is a procedure by which the most identifying fields within a data set are replaced by one or more artificial identifiers, or pseudonyms

As technology continues to develop rapidly and the EU embraces Big Data, the importance of enhancing data protection rights and principles grows exponentially. Consumers can expect individual and collective benefits from the development of Big Data technologies and applications but ONLY if a solid legal data protection framework is established now to protect their fundamental right to privacy. Such a solid framework is essential for consumers' trust in the Digital Single Market.

Consumers are not commodities, their rights must be protected and their personal data should be nobody's business but their own.

KEY CONSUMER DEMANDS FOR THE GENERAL DATA PROTECTION REGULATION TRILOGUE

1. The definition of personal data must cover any kind of information that would allow to identify an individual or single someone out as an individual, including pseudonymous data

The definition of personal data is crucial in terms of defining the scope of the Regulation. In an interconnected digital world, individual pieces of data cannot be regarded in isolation. In order to ensure the new data protection rules remain relevant in years to come, the definition of personal data should remain broad and flexible in light of the rapidity of ICT developments.

- *As a general principle, the definition of personal data must cover any kind of information that would allow to identify an individual or single someone out as an individual. Recital 24 and Article 4.1 must clearly reflect this.*

- *Pseudonymous data shall not be defined as a separate category of data in article 4.1, it is by definition personal data and falls under the scope of the Regulation. Pseudonymisation should be encouraged as a means to provide an extra layer of security and protection, in no way should it open the door to unjustified exemptions.*

2. The "purpose limitation" and "data minimisation" principles must not be weakened

The principle of purpose limitation is one of the crucial pillars of the data protection legislation. It is particularly important given the proliferation of business models which are constructed on the basis of data sharing with third parties for purposes different to those initially pursued by the data controller e.g. a search engine or shopping website that share data with advertisers, and often without informing the data subject. Therefore, personal data must only be collected and processed for specified, explicit and legitimate purposes, which are to be communicated to the data subject. Further processing of data for purposes different to the original must only be allowed if the new purposes are compatible with the original ones. For example, if a consumer buys groceries or orders food online the information related to what he buys should not be processed for other purposes, such as assessing his eating habits in order to calculate the cost of his health insurance premium.

Moreover, a strong data minimisation principle is necessary in order to address the current trends of data harvesting and data mining used for profiling consumers.

- *Article 5c should be kept as in the Parliament position and the original Commission proposal, clearly stating that the amount of personal data processed must be limited to the minimum necessary and that personal data shall only be processed if the purposes pursued could not be fulfilled by processing information that does not involve personal data.*

- *Article 6.4 of the Council's General Approach must be deleted in its entirety. It legalises processing for incompatible purposes to the point of almost rendering the whole Regulation meaningless. If this article is kept, there would be almost no limits to what a company could do with the personal data it collects.*

- *Article 6.3a of the Council's General Approach provides criteria for assessing what could be considered compatible processing. The notion of compatibility is crucial. If maintained, this article shall be drafted and interpreted in a strict manner. Introducing an open-ended list of criteria would undermine the purpose limitation principle. Also important to point out that consumers should be informed when the data controller is using their personal data for purposes other than the original. Otherwise they would lose control of how and when their data is processed and the entire system of protection will become opaque, weak and unstable.*

3. The concept of "legitimate interests" as a legal basis for data processing must be narrowly defined and only used exceptionally

The legitimate interests of the data controller are possible grounds for lawful processing under article 6.1f. In practice companies are using "legitimate interest" as a basis for unrestricted and unregulated processing of personal data without user control, evading compliance with data protection principles. Therefore, unless narrowly defined and only used exceptionally, processing on the basis of "legitimate interests" will become a loophole in the new Regulation. This aspect is also particularly important as companies will probably try to use the "legitimate interests" ground as much as possible in the context of big data analytics.

- *Strict criteria for the interpretation and application of the "legitimate interests" ground are necessary. Article 6.1f should state that it should only be possible to use "legitimate interests" as a last resort i.e. when no other legal grounds are available. Also, if a data controller wishes to use this ground for processing, this must be flagged to the data subject. The data controller should also be required to publish the reasons for believing that its interests override those of the data subject.*

- *The European Data Protection Board should be entrusted with the task of publishing an indicative lists of processing operations which can be based on the legitimate interests of companies. "Direct marketing purposes" should not be considered as being generally covered by the "legitimate interests" ground.*

4. Provisions on processing of personal data for scientific, historical and statistical purposes must be clarified and not understood as a separate legal basis for processing

While BEUC understands and supports the need for specific provisions to avoid hindering the processing of personal data for scientific, historical and statistical purposes in the public interest, we believe that the Council's General Approach does not provide sufficient safeguards to prevent companies from exploiting such provisions for commercial purposes.

- *The Regulation must properly define what is understood by scientific, historical and statistical purposes and under which conditions special provisions apply. In particular, these purposes must be explicitly limited to research activities, in line with the European Parliament's proposal. Particular attention is needed to prevent private companies from misusing these provisions, for example by presenting profiling activities as data processing with merely statistical purposes.*

- *Article 6.2 must not constitute a separate legal basis for processing. The wording of this article should clearly indicate that processing of personal data for scientific, historical, statistical and archival purposes should always be based on one of the legal grounds included in Article 6.1, such as consent, processing for the performance of a contract to which the data subject is party, or for the performance of a task carried out in the public interest.*

- *Articles 9.2i and 83 of the Council General Approach must be carefully reviewed to limit to the minimum necessary the possibilities to restrict the rights of the data subjects when their data is processed for scientific, historical or statistical and purposes, in particular when it comes to sensitive data.*

5. Controllers must be required to provide clear and comprehensive information to data subjects in a transparent and timely manner

The Regulation indicates what information and notifications the data controller is obliged to give to the data subject when his or her personal data is collected and used. This kind of information must be comprehensive and easily accessible in order to ensure maximum transparency towards consumers, facilitating their understanding in relation to why and how their data is being used, making them aware of their rights and allowing them to make informed choices. For example, services whose business model is based on monetising the use of consumers' personal data in exchange for so-called 'free services' should make it crystal clear in the information they provide to the consumer that this exchange is taking place.

- *In line with Articles 11, 12, 13a and 14 of the Parliament's position, the controller should provide comprehensive and easily accessible information about the type of personal data collected and processed, for which purpose, the legal basis for processing, the retention periods, whether the data is shared, sold or rented out to commercial third parties, the rights of the data subject (how to exercise the right to complain and seek redress), actions taken under the request of the data subject, etc. In particular, the data subject shall be informed about tracking and profiling activities and their possible consequences.*

6. The right to data portability must be broad and be kept as a separate right from the right to access

The right to data portability laid out in Article 18 is essential to empower consumers and ensure that they are not 'locked in' to certain services or platforms. This right allows consumers to be in control and retain the ownership of their personal data by being able to transfer it to other services.

- *Article 18 shall be amended so that the right to data portability applies to all types of processing. Exercising this right should also imply the erasure of the data no longer needed by the original service provider, in line with the European Parliament's position.*

- *Moreover, Article 18 should also state that the data should be provided to the data subject in an interoperable format. It should also give the data subject the possibility to request the transfer of the data directly from one controller to another, in line with the Parliament's position.*

7. The provisions on profiling must be strengthened and must include a clear right to object to being profiled

Profiling consists of the collection and use of personal data in order to be able to predict how an individual behaves. Predictions are made using automated mechanisms (algorithms) and can be used for profit purposes. However, regardless of what their final use is in the end, consumer profiles already have standalone economic value by themselves. These profiles are often created without the consumer's knowledge, who is rarely informed of profiling techniques nor the logic behind them or their consequences. In the meantime, different actors are tracking and analysing consumer's every move online, creating very detailed profiles which are sold to the highest-bidder and used for various commercial purposes such as marketing and advertising. Measures based on profiling can also result in different sorts of discrimination (racial, ethnic, economic, etc.). For example, an online retailer could make a consumer pay a higher price for a product based on his financial means, social status, online activity and personal needs or preferences, which the retailer knows from the consumer's purchasing history and a profile of the consumer that has been built up and sold by a data broker.

The Regulation should put an end to opaque profiling practices and prevent discriminatory situations by introducing rules dealing both with the collection of data for the purpose of profiling, i.e the creation of profiles as such, and with automated decisions based on profiling, in line with the European Parliament's position on Article 20.

In general, greater transparency and user control is needed when it comes to profiling. Weak provisions on profiling, coupled with watered down data minimisation and purpose limitation principles and with unrestricted data processing based on legitimate interests would be a worst case scenario with devastating effects for data subject's privacy. In particular, Article 20 should include the following elements:

- *Consumers must have the right to object to the processing of their personal data for profiling purposes.*

- *There must be provisions defining the purposes for which profiles may be created and used, including obligations to inform consumers that they are being profiled, the techniques used, the possible consequences of that profiling and that they have the right to object to the creation and use of the profiles.*

- *The "legitimate interests" of the controller or a third party cannot be accepted as a legal ground for profiling.*

- *Data subjects should also have the right to access, to modify or to delete the profile information attributed to them.*

- *Profiling of vulnerable consumers such as children should be prohibited.*

8. The principles of "data protection by design and by default" are key to help empower data subjects and must not be watered down

Introducing "Data protection by design and by default" will help limit the collection of personal data and enhance consumers' trust that their data is protected. It will ensure that even non-digital consumers who are unfamiliar with privacy settings of services and products will have protection.

Privacy settings are a very important aspect of online privacy. Consumers expect companies to create privacy settings that provide transparency and control over the ways in which personal information is collected, used and stored. For example, consumers should be able to trust that a fitness tracker comes with a default setting preventing the device from accessing personal data which is unnecessary for its core functions.

- *Article 23 shall make it compulsory for data controllers to implement appropriate measures to comply with the principles of "privacy by design and by default". In particular, it should be explicitly mentioned that consumers' personal data shall be respected all throughout the lifecycle of products and services.*

- *Also it should be clearly stated that the privacy settings on services and products shall by default comply with the general principles of data protection, such as data minimisation and purpose limitation.*

9. There must be a dual system of notification of personal data breaches with a general principle that all breaches must be notified to the Data Protection Authorities

Giving too much leeway to data controllers when it comes to breach notification, leaving them to assess solely by themselves what is serious or not and whether they should notify, could result in major breaches not being notified either to the Data Protection Authorities or to the data subjects. For example, a bank offering online services could find out that due to a breach the card information of a customer has been stolen. However, the customer does not have much money in his account and the card will expire in the coming days, so the bank could consider that risk that the customer would negatively be affected is low and decides not notify the breach to the supervisory authority or the consumer. The consumer would then remain in the dark about the breach of his personal data.

- *As a principle, Articles 31 and 32 shall involve that all breaches should be notified to the data protection authorities while only those breaches which entail high risk to the data subject should be notified to individuals, in line with the European Parliament's position.*

- *Moreover, taking subsequent measures to ensure that the high risk for the data subject is no longer likely to materialise should not relieve the data controller from the obligation to notify. Therefore, Articles 31.1a and 32.3b of the Council General Approach shall be deleted.*

10. Consumers shall have access to effective redress mechanisms. Organisations defending the interests of data subjects shall have the right to take legal actions both on behalf of data subjects and independently

When data protection rules are infringed consumers must be able to effectively seek redress and be compensated for the damage they have suffered. Infringements often affect more than one individual and legal actions can be lengthy and expensive. It is crucial that consumer organisations and other associations defending the rights of data subjects can act on behalf of an individual data subject or a group of them. Allowing collective legal actions is important as it makes it easier and less cumbersome for consumers to access redress and be compensated for the damage they suffer.

Moreover, consumer organisations shall be allowed to bring actions to court independently of a data subject's mandate, if they consider that the rights of a data subject have been violated as a result of the processing of personal data which is not in compliance with the law. This is also an important piece of the enforcement puzzle and will serve as a solid complement to the enforcement activities of the Data Protection Authorities.

- *In line with the European Parliament's position, Article 76.1 should include the possibility for consumer organisations to carry out actions to seek compensation for damages if mandated by an individual or a group of consumers.*

- *In line with the Council General Approach, Article 76.2 must allow a consumer organisation to take legal action independently of a data subject's mandate if it considers that the data protection rules have been infringed. However, the Council text should be amended to make this provision binding for all Member States to ensure an equal level of protection all across the EU.*

END

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