BEUC The European Consumer Organisation

The Consumer Voice in Europe

Justice Council meeting 15 June – Council General Approach on the General Data Protection Regulation

Letter sent to the Ambassadors 11 June 2015

Contact: **david martin– digital@beuc.eu**

Ref.: BEUC-X-2015-059 - 11/06/2015

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • Fax +32 (0)2 740 28 02 • consumers@beuc.eu • www.beuc.eu
www.twitter.com/beuc - EC register for interest representatives: identification number 9505781573-45

Dear Ambassador,

I write on behalf of the European Consumer Organisation (BEUC) to draw your attention to a number of important unresolved issues regarding the proposal for a General Data Protection Regulation (GDPR), in light of the upcoming meeting of the Justice Ministers on 15 June.

We welcome the progress achieved so far under the Latvian Presidency and are hopeful that the Council will reach a general agreement on the whole text of the GDPR at the meeting next week. Nevertheless, we are concerned that in some important cases the direction taken in Council deviates from the original purpose of the reform and the principles that should be guiding it.

We are in particular worried about opening the door for unrestricted processing of personal data based on "legitimate interests" of the data controller or a third party as well as about lowering the threshold for allowing profiling of data subjects. We underline the importance of enabling consumer organisations to efficiently defend the interests of consumers in case of infringements. A list of our main concerns is attached to this letter.

Technology is developing rapidly and fundamentally changing our society in the process. Data, in particular personal data, has become a commodity in the Digital Age, and its value is only likely to increase as we move into a Big Data driven economy. From a consumer viewpoint, it is unacceptable that the data protection reform is taking so much time, given the urgent and overdue need to enhance consumers' rights and put them back in control of their own personal data.

Companies operating online and particularly those whose businesses models are based on the collection and processing of consumers' personal data must be subjected to a legal framework built on solid data protection principles, wide-ranging data subject rights and effective enforcement mechanisms. We must not forget that the protection of personal data is a fundamental right.

A robust data protection legal framework is essential to boost consumer trust in the Digital Single Market, as evidence shows that *70*% of *Europeans* are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected and 67% believe that there is no alternative to disclosing personal information if one wants to obtain products or services. Additionally, the data protection reform will also provide businesses with a coherent and comprehensive legal framework to work across Europe.

All this makes the GDPR a key pillar if we are serious about building a truly functional Digital Single Market that allows consumers and businesses to fully reap the benefits of the digital economy.

Protection of personal data and economic growth are not contradictory. We must find the right balance between creating an effective system of data protection for EU consumers and avoiding excessive administrative burden for companies. But in doing so we must not forget that the EU is, and should continue to be, the world leader when it comes to the highest standards for privacy and data protection.

We therefore urge you to take the consumers' perspective into consideration when agreeing on a general approach next week and during the trialogue negotiations with the European Parliament. In the meantime, we remain at your disposal to provide further information.

END

ANNEX – Key consumer demands for the GDPR

BEUC has identified below a number of issues that the Council must consider in its general approach and during the trialogue negotiations with the European Parliament.

1) The definition of personal data must remain broad and flexible

In order to ensure that 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. This definition must cover any kind of information that can personally identify an individual or single them out as an individual.

Re-identification and "de-anonymisation" of personal data are increasingly common malpractices. Full anonymisation is increasingly difficult to achieve with the advance of computer technology and the vast availability of information. The processing of data rendered "anonymous" should still require compliance with the fundamental principles of data protection, such as data minimisation and purpose limitation, given that full anonymisation can never be assured.

2) The principles of purpose limitation and data minimisation should not be diluted by the legitimate interests of the data controller or third parties

Of particular concern are some of the provisions in articles 5 and 6 relating to the principles and the lawfulness of data processing.

The principles of purpose limitation and data minimisation are crucial pillars of the data protection legislation. Article 5 should clearly state that personal data collection and processing should be limited to the "minimum necessary". Furthermore, personal data shall only be processed if the purpose for which the data is processed cannot be fulfilled by processing information which does not involve personal data.

Article 6.4, which allows for personal data to be processed for purposes that are incompatible with those that justified the initial collection of the data, based on the shaky legal grounds of "legitimate interests of the data controller or a third party", would basically render the whole Regulation void of any meaning. This is absolutely unacceptable.

We accept that the legitimate interests of the data controller are possible grounds for lawful processing. However, companies use this as a basis for the unrestricted and unregulated processing of personal data and not allowing user control. Unless properly defined and used only exceptionally, the legitimate interests of the controller as a legal base for justifying data processing (even incompatible processing!) will certainly become a high-speed lane for circumventing the new Regulation.

Also, the list of criteria to define compatible purposes for data processing laid out in article 6.3 must be clear and exhaustive to avoid legal uncertainty and loopholes in the Regulation.

3) Data subjects' rights must be robust and comprehensive. Restrictions of these rights should be as targeted as possible and limited to specific causes

Data subjects' rights such as the right to object, the right to data portability, the right to access personal data held by the controller and the right to deletion of the data, are at the core of the reform and must not be undermined.

Restrictions to user rights should be limited and include sufficient guarantees in relation to the purposes, proportionality, necessity, categories of data processed and the persons authorised to carry out the restrictions. Administrative or economic burdens should not be a valuable justification for the restriction of rights.

4) The provisions on profiling and the right to object must be strengthened

The change in the title of section 4 and article 20 is a small but significant illustration of the Council's misguided approach to some of the key provisions of the Regulation. Replacing the word "Profiling" with the expression "Automated Decision Making" is confusing to say the least.

Profiling and Automated Decision Making (which can be based on the results of profiling) are two different things. The right to object must include the right not to be subject to profiling. Moreover, consumers should be informed of profiling techniques and procedures, as well as of their consequences. Profiling of vulnerable consumers, such as children, must be explicitly prohibited.

5) All data breaches must be notified to the data protection authorities

BEUC supports the dual system of notification under which all data breaches must be notified to the data protection authorities, while only those breaches that risk in any way to adversely affect the protection of personal data and privacy should be notified to individuals.

The risk assessment of a data breach should not be placed solely in the hands of companies. Also, the fact that a controller has taken measures to ensure that the risk is no longer likely to materialise should not exempt from the obligation to inform the data subject.

Furthermore, the risk of a breach of pseudonymity is an element that should be taken into account when evaluating the importance of a data protection breach and when carrying out a data protection impact assessment (articles 32 and 33).

6) Codes of conduct and certification mechanisms must not open the door to uncontrolled data transfers to third countries

According to the latest drafts of the Regulation, simply by signing up to an "approved" code of conduct, a company that is not subject to the Regulation could provide appropriate safeguards within the framework of personal data transfers to third countries. If such a system of "approved" codes of conduct and certification schemes is maintained without appropriate coordination and oversight, BEUC is concerned that it could be used to allow data transfers to third countries without adequate protection. Moreover, no transfer of personal

data to authorities of third countries should take place without prior approval by data protection authorities.

7) Consumer redress - the role of consumer organisations and associations defending public interest is key to guarantee effective enforcement of data subjects' rights

When data protection rules are infringed data subjects should be able to seek redress and effectively be compensated for the damage they suffer. For this to be feasible it is crucial that consumer organisations or associations defending data subjects' rights can lodge complaints or seek actions in court on behalf of an individual data subject or a group of them (article 76). This right to act on behalf of data subjects should include judicial actions for compensation and should be possible even if the statutory objectives of the association or organisation in question do not specifically include data protection, as long as the general protection of data subjects' rights and freedoms is without a doubt the main overall objective of the association.

This is important as often the value of the damage caused to an individual is not worth a lengthy and expensive legal action. By allowing collective legal actions, it will be easier and less cumbersome for consumers to access redress and be compensated for the damage they have suffered. This will also complement the enforcement actions carried out by the Data Protection Authorities, ensuring that data subjects have access to all possible effective redress mechanisms.

The possibility for Member States to allow organisations or associations defending data subjects' rights to lodge complaints before a supervisory authority and bring actions to court, independently of a data subject's mandate, should also be maintained (Article 76.2). Ideally, to ensure a harmonised level of consumer protection all across the EU, this provision should be strengthened by making it an obligation for Member States to introduce this possibility.

8) The principle of joint liability for the data controller and the data processor should be maintained. Sanctions in case of non-compliance must be strong and dissuasive

The general principle of joint liability of the data controller and data processor is important in order to allow data subjects to easily seek redress, as it might be difficult for them to determine which entity is the data controller and who bears the liability in case of damages.

It is crucial to establish a robust sanction mechanism in case of infringements, similar to the one that exists under competition law. Failure to do so could result in systematic disregard of the rules established in the Regulation, especially by commercial entities with strong economic and market power. The lack of such a mechanism has been one of the weaknesses of the current regime and it is important to correct this situation. Furthermore, BEUC proposes that the fines imposed on companies could be used, at least in part, to finance the actions of organisations defending the rights of data subjects.