BEUC The European Consumer Organisation

The Consumer Voice in Europe

EU DATA PROTECTION DAY - KEY MESSAGES

Contact: **Konstantinos Rossoglou – digital@beuc.eu**

Ref.: X/2013/007 - 28/01/2013

Happy EU Privacy Day: Personal data must belong to the consumers

This year, the celebrations for the European Privacy Day coincide with the revision of the EU data protection framework.

Consumers across Europe expect their elected European Parliamentarians to ensure existing data protection standards in the EU are not weakened and the revision of the legal framework restores consumers' control over their personal data. This is all the more important in an ever more complex online environment where individuals' fundamental right of personal data protection is being violated - unknown to consumers.

Consumers currently live in a digital 'dark room' in terms of control over the way information including their identity, daily lives, social activities, political views, hobbies, financial data and health records are collected and processed by multiple companies. Billions of euro are made each day by "flourishing" companies (ab)using our personal data.

Existing surveys indicate that consumers are growing increasingly suspicious of the ways their personal data is handled by companies in the digital era:

- 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;

- 43% of Internet users in the EU say they have been asked for more personal information than necessary when they wanted to access or use an online service;

- 67% believe that there is no alternative to disclosing personal information if one wants to obtain products or services.

The right to the protection of personal data should not be eroded or undermined simply because it became easier or more profitable to break it in the digital environment.

There are not many issues on which Europe currently has global leadership. But the protection of personal data is one such example. The European legal framework for the protection of personal data has become a model around the world, having a huge impact on other continents and countries - many have reformed their national laws according to the European standards.

We should all be proud of this and endeavour to continue defend our standards against the proliferation of new (and not so new) business models based primarily on the (ab)use of our personal data.

The processing of personal data knows no borders. Therefore, the revision of the data protection framework in Europe may have an impact on the lives of consumers and citizens around the globe. This is a huge current challenge for the EU right now. Members of the European Parliament should not miss this opportunity - the Parliament should stand firm against the many industry demands to weaken the rules proposed by the European Commission.

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
EC register for interest representatives: identification number 9505781573-45

Indeed, many misleading messages and misconceptions have been heard since this "battle" started. Let's dismantle some of them:

- **Protection of personal data and economic growth are not contradictory**

Consumer confidence is essential to economic recovery. According to the Eurobarometer survey (No. 390), a lack of consumer trust acts as a significant barrier to the development of e-commerce and the digital economy.

A solid legal framework for data protection would help boost consumer confidence, especially in the complex online environment. Innovation will only be able to be rolled out on a large scale if people trust the way their data is being handled.

The proposal for a Regulation on Data Protection strikes the right balance between, on one hand the need for an effective system of data protection, and on the other for businesses not to be confronted with excessive administrative burdens. To reduce administrative burdens the draft regulation has abolished the (burdensome) notification procedure which costs businesses about €130 million per year, according to the European Commission's Impact Assessment.

Yet, lesser administrative burden should not result in weaker protection of personal data nor limit companies' liabilities *vis-à-vis* data subjects. On this theme, the draft regulation establishes the principle of accountability according to which the data controller will adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the Regulation.

In addition, the draft Regulation will create a level playing field for businesses via a single law applicable to any business across the EU. This harmonisation is expected to save businesses up to €2.3 billion per year, according to the European Commission's Impact Assessment.

Companies operating in the EU will also be answerable to a single data protection authority (DPA), no matter how many EU countries they do business in.

- **Strong data protection is a competitive advantage for Europe**

The draft Regulation will extend the application of EU data protection rules to all companies who offer goods and services to European consumers or who monitor their behaviour.

Article 3 on territorial scope will create a level playing field for both EU and non-EU companies when they process the personal data of European consumers. As a matter of fact, EU companies will have a competitive advantage as they are already familiar with the strong data protection rules across Europe. The burden will be on companies from third countries.

The introduction of an explicit right to data portability in the draft Regulation will also stimulate competition. By allowing consumers to switch providers, the draft regulation will facilitate market entry for new, innovative companies. In fact, presently consumers are too often 'locked-in' to online services and platforms

with no possibility of transferring their data to other competing platforms e.g. e-mail services, social networks etc.

The argument of companies that the right to data portability is incompatible with intellectual property rights is misleading, as the right to data portability only applies to data provided by the consumer himself or data which has been collected in the framework of a contractual relationship and therefore the consumer should be able to retrieve this data once the contract is terminated.

Article 18 on data portability must be maintained as a separate right. A similar right to number portability already exists in the telecommunications sector and is a key aspect of competition.

- **The draft Regulation will *not* stifle innovation**

Over the last 12 months, there has been a huge degree of misinformation on the proposed Regulation. Businesses argue that the proposed Regulation will alter the way the internet works and will hinder innovation.

These arguments are put forward by those companies, mainly from the US, who have a long tradition of not complying with EU data protection laws. The draft Regulation specifies the principles for processing personal data which already exist in the Directive 95/46 and strengthens the rights of individuals that are already embedded in EU law. The right to information, the right to access, the right to object, the right to correct and erase are not new rights.

Companies have simply not bothered to comply with the existing law.

- The Article 29 Data Protection Working Party has recently launched investigations into the practices of Google and Microsoft with regards to their new privacy policy.

- Consumer organisations from both sides of the Atlantic also asked Google to delay the entry into force of its new privacy rules until consumer advocates had the time to provide feedback. However, Google ignored our request.

- Facebook has denied access to the personal data collected and retained of its users and has preferred to engage in litigation against a law student from Austria who wanted to exercise his existing rights in a test case.

Once the new rules are in place, the application and enforcement of the rights of consumers will improve; enforcement bodies will be able to deploy more resources and strong sanctions for non-compliance will be introduced acting as a deterrent. Law abiding companies have nothing to fear.
There are a number of issues which in our view are absolutely essential to preserve current standards and allow consumers to remain in control of their data in an ever changing technological environment. Surprisingly, these issues are also some of the most controversial in the recent parliamentary committee opinions.

1. Definition of personal data

In order to ensure that the new data protection rules will remain relevant in years to come, the definition of personal data should remain broad and flexible in light of the rapidity of ICT developments.

Article 4 reiterates the existing definition of the Directive 95/46 and further clarifies that 'online identifiers' and 'location data; are personal data when they are related to an individual. (Online) identifiers should, as a rule, be considered personal data.

The definition must be clarified to ensure any information which can be used to single out a person qualifies this information as personal data. In many applications, identifying a natural person is not needed to have an adverse effect on the person; "singling out", i.e. the possibility to distinguish the person from other persons in a group, is very often enough to define the profile of an individual. This interpretation is particularly relevant in relation to profiling techniques used in the internet eco-system.

With regards to **anonymous data**, it must be borne in mind that it is almost impossible to ensure full anonymisation of personal data. It is therefore important that the processing of data rendered 'anonymous' would still require compliance with the fundamental principles of data protection, such as data minimisation and purpose limitation, given that full de-anonymisation can never be ensured.

Pseudonymous data are in principle identifiable and therefore should not be excluded from the scope of the Regulation. It is equally important that the rights to access and deletion continue to apply to such data.

2. Consent

Consent of the data subject is one of the possible criteria which can legitimise data processing and therefore constitutes a fundamental element of the data protection legislation and an important tool of data subject's empowerment. Currently, consumers' consent is presumed to be given with the ticking of a box at the end of an unclear, legalistic privacy notices written by lawyers for lawyers. Consent is being abused by companies who mislead the consumer to agree to processing his/her personal data, in clear breach of the law.

Consent may not be the appropriate legal ground in all cases. For example if there is an imbalance between the individual and the company or most importantly, when the consumer does not have a choice but to agree, as is the case when a company holds a dominant position in a specific market.

It is important to ensure that when businesses decide to rely on consent, the conditions for consent are strict and businesses should bear the burden of proof that the requirements have been met.

3. Legitimate interests

The legitimate interests of the data controller, is one of the six grounds for lawful processing. Companies have served this ground as a basis for unrestricted and unregulated processing of personal data without allowing any user control. Google has based its revised privacy policy, by which users "grant" Google a *carte blanche* to combine almost any data from any services and for any purposes. Google's privacy policy is under investigation by Article 29 Data Protection Working Party.

Many companies use 'legitimate interests' to collect more data than is required, often for different and incompatible purposes than the initial purpose. The legitimate interests ground is often used as a pretext to pass data on to third parties and escape compliance with the principles of data protection.

Therefore, unless properly defined and only used exceptionally, the legitimate interests of the controller will become the loophole of the new Regulation. If a data controller wishes to use 'legitimate interest' as a basis for processing, this must be flagged to the data subject and the data processor should publish its grounds 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 list of processing operations which can be based on the legitimate interests of companies.

4. Breach notification

Individuals have the right to be informed about the use of their personal data, including when their data has been compromised. According to the research carried out by our UK member organisation Which?, the vast majority of UK consumers (74%) would always wish to be notified of a data breach.

BEUC supports the dual system of notification established in the draft Regulation, according to which all breaches must be notified to the Data Protection Authorities while only those breaches which adversely affect the protection of personal data and privacy should be notified to the individuals.

Such a dual system prevents "notification fatigue" of data subjects and ensures data controllers cannot escape from the responsibility to notify of a breach.

On the contrary, restricting notification to the supervisory authority only to serious breaches, would put controllers in a position to decide themselves what is serious or not. There is the risk that major breaches will never be notified to the detriment of consumers' personal data.

END