BEUC The European Consumer Organisation

The Consumer Voice in Europe

PEOPLE OWN AND MUST BE ABLE TO CONTROL THEIR PERSONAL DATA

BEUC key demands on the Proposal for a General Data Protection Regulation

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

Ref.: X/2013/027 – 23/04/2013

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

GENERAL ISSUES

PEOPLE OWN AND MUST BE ABLE TO CONTROL THEIR PERSONAL DATA

Consumers currently live in a digital 'black out' in terms of how information on their identity, daily lives, social activities, political views, hobbies, financial data and health records is collected and processed by a multitude of companies. Billions of euro are made each day by "flourishing" companies (mis)using our personal data.

Existing surveys indicate that consumers do care about the way their personal data is being used and they 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.*
>
> Only 26% of those surveyed feel that businesses are sufficiently transparent in how they use personal data, while a definite majority - 75% - describe regulation preventing misuse of such information as "weak"[1].

The objective of the reform is to strengthen existing rights and principles while restoring consumer control over the way their personal data is processed. However, the majority of companies, from advertising to the tobacco industry, have seen it as an opportunity to water down the existing level of protection of personal data in the EU.

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

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

A solid legal data protection framework would help boost consumer confidence, particularly 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 handled.

[1] "Privacy uncovered.Can private life exist in the digital age?" http://www.managementthinking.eiu.com/sites/default/files/downloads/Privacy%20uncovered_0.pdf

MEMBERS OF THE EUROPEAN PARLIAMENT CAN BECOME PRIVACY CHAMPIONS

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

There are a few issues on which Europe currently has global leadership. The protection of personal data is one such example. European data protection laws have 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 (mis)use of our personal data.

One year before the next European elections, 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.

RISK-BASED APPROACH

The data protection framework should apply to all processing of personal data and not only to the risky ones. Risk is inherent in any data processing. For example, the obligation to carry out a Data Protection Impact Assessment consists of identifying the risks related to a specific data processing operation. Excluding from the scope of this obligation a priori operations which might seem less risky on the face of it, is likely to weaken protection, to the detriment of data subjects.

Furthermore, from the amendments tabled it remains unclear who will be responsible for defining the risk of specific processing operations. It cannot be left to controllers as to whether they have to comply with the more stringent obligations under the draft Regulation. Whereas the principle of accountability should be clearly outlined in the text of the Regulation, it should not result in completely removing certain controller's obligations.

The accountability principle might be more appropriate for large multinationals having the necessary human and financial resources to implement comprehensive privacy programs, but is less appropriate for Small and Medium-sized Enterprises which require a checklist to ensure compliance with their obligations under the Regulation.

SPECIFIC ISSUES

DEFINITION OF PERSONAL DATA

The definition of personal data is crucial in defining the scope of the draft 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 clearly stated by the Article 29 Data Protection Working Party2, re-identification and de-anonymisation of personal data is an increasingly common malpractice. Full anonymisation is an illusion and increasingly difficult to achieve with the advance of computer technology and the vast availability of information.

> *In 2006, a study found that if you know how a user rated just six films, it is easy to identify 99% of the users in Netflix database[3].*
>
> *A study found that it is possible to identify 87% of Americans using only three pieces of information, namely ZIP code, birth date (including year), and sex[4].*

ANONYMOUS DATA

When personal data is irreversibly anonymised, they automatically fall outside the scope of the Regulation. A definition of "anonymous data" should be avoided, since such a definition would increase the risk of creating loopholes. Such flaws could then be exploited by controllers to circumvent the rules of the Regulation.

PSEUDONYMOUS DATA

Pseudonymised data is by definition personal data as it relates to an identifiable individual and therefore falls within the scope of the draft Regulation. BEUC regrets that a number of amendments have suggested making pseudonymisation - which is simply replacing the name and other direct identifiers with a new identifier (i.e. person 2454548)- a sufficient reason to make data processing legitimate, and exempt the processing of pseudonymous data from core data protection principles.

On August 3, 2006, America Online (AOL) posted on a public website twenty million search queries for 650,000 users of AOL's search engine. Before releasing the data to the public, AOL had tried to anonymise it to protect privacy, by suppressing any obvious identifying information such as AOL username and IP address and replacing them with unique identification numbers in the released data. In the days following the release, bloggers and journalists managed to identify specific individuals.

[2] Opinion 03/2013 on purpose limitation, adopted on 2 April, 2013.
[3] Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets, in PROC. OF THE 2008 IEEE SYMP. ON SECURITY AND PRIVACY 111, 121.
[4] 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', University of Colorado Law School, August 13, 2009

PURPOSE LIMITATION AND COMPATIBILITY OF FURTHER PROCESSING

The principle of purpose limitation is one of the crucial pillars of the data protection legislation. The data controller has the sole obligation to collect and process the personal data 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 is only allowed if the new purposes are compatible with the original ones. However the notion of compatibility is not defined in the proposal. It is thus important that certain general criteria are put forward to be used to assess the compatibility of further processing.

BEUC proposes that the task of setting such criteria is entrusted to the European Data Protection Board. The recent Opinion by the Article 29 Data Protection Working Party already provides a basis:

- the relationship between the original purpose and the purposes of further processing;
- the context in which the data were collected; the reasonable expectations of the data subject;
- the nature of the data and the impact of further processing on the data subject; and
- the safeguards applied by the controller to prevent any undue impact on the data subject.

Furthermore, should the data controller use and process personal data for purposes other to the original without informing the data subject, consumers will lose control of how and when their data is processed and the entire system of protection will become opaque, weak and unstable.

An online shop selling electronic appliances, collects and processes personal data (such as your name and address) for the purpose of sending the appliances you bought to your home. Subsequently, the online shop uses the same data to send you advertisements and marketing material at home. Such further processing is incompatible with the original purpose for which your data was collected.

LEGITIMATE INTERESTS

The legitimate interests of the data controller are possible grounds for lawful processing. However, companies have used this as a basis for unrestricted and unregulated processing of personal data and without allowing user control:

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

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 interests' as a basis for processing, this must be flagged to the data subject;
- The legitimate interests ground can only be used as a last resort i.e. when no other legal grounds are available;
- The data controller should prove 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.

Google has based its newly revised privacy policy on its "legitimate interests"; Google's users have no option but to accept the new privacy policy if they want to use its services. However, with its revised privacy policy Google has allowed itself to use, process and_combine almost any data from any service and for any purpose without adequately informing its customers. The legality of the Google's new privacy policy is in fact being challenged by data protection authorities across the EU.

DATA PORTABILITY

BEUC welcomes the introduction of the right to data portability in the draft proposal. The right to the portability of personal data is essential to ensure consumers are not 'locked in' to certain services or platforms, by becoming captive consumers.

In particular online, certain online platforms which store and process personal data (mail, photographs…) do not allow their customers to access and transfer their personal data onto a different (competing) platform or service provider. This situation is incompatible with the right of consumers to be in control of and access their data. These limitations clearly hurt competition and should not be allowed.

In April 2013, the German social network 'SchülerVZ' (modeled similarly to Facebook) announced its closure on April 30, 2013 and that all content and data of its users is to be completely and irreversibly deleted http://www.schuelervz.net/l/help

A friend tells you about a new online service which allows you to store, sort and manage your holiday photographs but which has lost some of your files. You decide you want to withdraw your photos form the platform that you are currently using and store them with a new platform. However, the initial storing platform does not let you access your photos to transfer them. As a consequence, the consumer is a "captive" of the initial service provider.

PROFILING

Profiling consists of the collection and use of personal data in order to find out how an individual behaves. It also is used to make assumptions on the basis of this behaviour and the information is then used to profit. The logic used to make these assumptions is called profiling algorithms.

The main problems with profiling are that consumers are rarely informed of these techniques nor the logic behind them and they are not given the right to object to such measures. Moreover, some of these measures can have negative effects on individuals and give rise to various forms of discrimination (racial, ethnic, economic…).

- When subject to profiling measures, consumers should be informed and of the possible consequences or effects this could have on them;
- Consumers should be able to object to the processing of their personal data for profiling purposes at all times;
- The possible legal grounds for profiling should be limited: the legitimate interests of the controller cannot be accepted as a legal ground for profiling;
- Profiling of vulnerable consumers such as children should be totally prohibited.

Example:
An airline collects and processes personal data for the purpose of selling airline tickets. The same data is then further used and processed to build profiles of customers who are prepared to pay higher prices (based on previous purchases). Then, this category are only offered certain products and do not have access to the whole range of available offers.

DATA BREACH NOTIFICATION

Individuals should be informed 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%) wish to always be notified of a data breach.

BEUC supports the dual system of notification of data breaches 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 individuals. Such a dual system prevents "notification fatigue" of data subjects and ensures data controllers cannot evade the responsibility to notify of a breach.

On the contrary, restricting notification to supervisory authorities 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, thus to the clear detriment of consumers' personal data.

A bank offering online services finds out that the card number of a client has been fraudulently used. As a result, an amount of money has been stolen from the account. However the bank thinks that the amount stolen is unimportant enough to notify this to the supervisory authority or the consumer. The consumer then remains in the dark about the breach of his data.

CONSUMER REDRESS

When data protection rules are infringed or personal data breached, data subjects should be able to seek redress and be effectively compensated for the damage they suffer. For this to be feasible it is crucial that consumer organisations or associations defending their rights can lodge complaints or seek actions in court on behalf of a group of consumers.

Often the value of the damage caused to an individual is not worth a lengthy and expensive legal action. By putting collective actions in place, it will be easier and less cumbersome for consumers to access redress and be duly compensated for the damage they have suffered.

- The right of organisations or associations defending data subjects' rights to lodge complaints before a supervisory authority (Article 73) and to bring an action to court (Article 76) on behalf of data subjects should be maintained;
- The right of organisations to bring judicial actions for compensation should be added in Article 77.

A bug in the security system of an internet service provider has caused the loss of series of data related to many clients. The harm caused to each individual is not significant enough to justify the costs of an individual legal action. As a result, the company gets away with the infringement and the affected individuals will not be compensated. If all affected consumers could go to court represented together by one organisation, it will be easier for them to be adequately compensated for the damage they have suffered.

END