'A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION'

European Commission's Communication

BEUC, The European Consumers' Organisation's response

Contact: Kostas Rossoglou – digital@beuc.eu
Ref.: X/2011/003 – 24/01/11

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Summary

The European Consumers' Organisation (BEUC) welcomes the European Commission's Communication. Overall, the Communication has identified the main challenges and the shortcomings of the current Framework that need to be addressed in the forthcoming revision. However, we would urge the European Commission to be more ambitious. In particular, BEUC has identified a number of key issues that need to be addressed in the forthcoming review of the Data Protection Directive:

Strengthen individuals' rights

The new framework needs to be user-centric and ensure that individuals remain in control of their privacy. To this end, we urge the European Commission to:

- Reiterate the need for a **broad and flexible definition of personal data** and provide clarification as to its interpretation;
- Introduce a **general transparency principle** and promote the use of **Transparency Enhancing Technologies** and support the development **of standard privacy notices**;
- Consider the introduction of a **horizontal data breach notification obligation** for serious data breaches and in line with a proportionality test;
- Strengthen the principle of data minimisation;
- Introduce **specific modalities for the exercise** of the right to access, correct and delete personal data;
- Ensure the effective implementation of the **right to be forgotten**
- Introduce the right to **data portability**;
- Clarify the rules on **meaningful consent** involving all stakeholders concerned;
- Establish a non-exhaustive list of **sensitive personal data**;
- Introduce **privacy by design** as an explicit, mandatory principle and promote the use of **Privacy Enhancing Technologies;**
- Establish **joint and several liability rules** between a business and a third party in cases of breaches;
- Adopt a **binding EU instrument for judicial collective redress to** allow data subjects to get compensation for the damages suffered.

Enhance the Internal Market dimension

BEUC shares the view that further harmonisation of data protection rules is necessary given the cross-border nature of data flows.

- However, **further approximation should not result in reducing the level of protection for data subjects** but should reflect the nature of data protection and privacy as fundamental rights;
- **EU data protection law should apply** to cases where services are directed at EU citizens in line with the criteria established by Article 29 Data Protection Working Party;
- The mandatory carrying out of **Privacy Impact Assessments** and their certification by independent parties will help to increase the accountability of data controllers;
- **Self-regulation has proven ineffective** to addressing effectively the challenges related to privacy

Global dimension of data protection

Since more and more processing operations take place in a global context, there is a need to consider actual implementation and enforcement of data protection legislation in third countries for the granting of **adequacy** and ensure that **international agreements** reflect the high EU standards.

Data Protection Directive: a success story

BEUC recognises that the current Framework, based on flexible definitions, technology neutrality and a principle-based approach has stood up well to time, allowing a high level of protection of personal data, while enabling the emergence of new services and the promotion of innovation. It has also been used as a global standard and provided the basis for the development of legislation in third countries.

BEUC has repeatedly referred to poor compliance and a lack of proper enforcement as the major problems related to the existing Framework. Compliance and enforcement need to become key components of the EU strategy in the field of data protection. We would also like to stress that the ongoing revision should not be perceived by private and public entities as an excuse to bypass the law when processing personal data of users and citizens.

The need for a new Framework

The forthcoming revision of the data protection legislation provides an opportunity to ensure coherent implementation and effective protection of data subjects' fundamental rights to protection of personal data and privacy.

The current principles need to be maintained and complemented with additional measures to ensure more effective protection, especially in light of constantly evolving ICT developments. The EU needs to have a consolidated general framework that will apply across the board, which could then be complemented by more specific rules if necessary.

The revision of the current Framework also needs to acknowledge the changes brought about by the Lisbon Treaty. In fact, both the European Charter of Fundamental Rights and the European Convention on Human Rights which recognise the fundamental rights to the protection of personal data and to privacy - will now need to be fully complied with by both the EU institutions and Member States, acting within the scope of the EU law.

I. Strengthening individuals' rights

1. Ensure appropriate protection for individuals in all circumstances

BEUC urges the European Commission to put data subjects at the forefront of the considerations on the forthcoming revision of the Framework Directive. The new Framework needs to be user-centred and ensure that individuals remain in control of their privacy in a world of rapid ICT developments. A high level of protection of personal data and privacy is not only required by the entry into force of the Lisbon Treaty, but it also constitutes a sine qua non condition for the achievement of the objectives of the EU Digital Agenda, which needs to be built upon consumers' trust in the online environment.

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu

New challenges

Digital information technologies and the emergence of new services, although beneficial to consumers, also represent a major challenge to consumers' personal data and privacy. ICT often leads to a proliferation of the amount of information collected, stored, filtered, transferred or otherwise retained. The risks to privacy therefore multiply.

In the digital environment, almost every communication leaves behind detailed footprints and the collection of personal data has become the default rule. Internet and mobile information appliances allow large quantities of personal data to be collected, while data mining tools are used to track the online behaviour of individuals and predict their presumed preferences. Individuals are using social networking sites to share information about themselves, their friends, their family and colleagues, while the emergence of cloud computing results in the potential for consumers to lose control over their data that can be hosted anywhere in the world.

In addition, the development of e-Health raises concerns as regards the secondary use of data collected for the purpose of providing treatment and the security of electronic health records. Furthermore, e-government systems typically contain large quantities of sensitive personal data, shared between government departments with the increased risk of security breaches and uses for secondary purposes. Moreover, governments are increasingly analysing and exchanging information on their citizens in response to fears over terrorist attacks.

Similarly, the challenges to personal data protection are also increasing in the offline world alongside the development of ICT. For instance, RFID chips are widely used on consumer products, while sensors with biometric and electronic identifiers are often used to link data to individuals[1].

Furthermore, while the deployment of smart meters for energy consumption, despite the improvements in the information supply chain, raises the disturbing possibility of consumers being tracked for different purposes and by different entities.

While technology will keep evolving with the emergence of new services and the impact of the transition towards the Semantic Web[2] is yet to be defined, privacy concerns will continue to arise, as privacy is inherent to human nature and human dignity. The need for a high level of privacy protection is heightened by the fact that we are just at the beginning of the Digital Age: no one has yet been born into it and matured into adulthood, and no one has yet experienced the aggregate effect of living a digitally mediated life over the course of ninety years[3].

---

1 Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Working Paper No 1: the challenges to European data protection laws and principles, Ian Brown, Oxford Internet Institute, University of Oxford.

2 Semantic Web is based on machine-readable information and builds on XML technology's capability to define customized tagging schemes and RDF's (Resource Description Framework) flexible approach to representing data. The Semantic Web provides common formats for the interchange of data (where on the Web there is only an interchange of documents).

3 J. PALFREY and U. GASSER, Born Digital, Basic Books, New York, 2008, page 62.

Consequently, the forthcoming revision must not result in a lower level of protection that would jeopardise the fundamental rights of individuals, citizens and consumers. On the contrary, the review is an opportunity to provide for effective protection of consumers' fundamental right to protection of their personal data and privacy and ensure proper enforcement of the rules.

Need for a broad definition of the concept of personal data

BEUC supports a wide definition of personal data, as already included in the Data Protection Directive[4] and interpreted by the Article 29 Working Party[5]. This definition provides the necessary flexibility to be applied to different situations and developments affecting fundamental rights, including those not foreseeable at the time of the Directive's adoption. This is all the more relevant in light of rapid ICT developments. Responding to criticism as regards the broad definition, Article 29 has specifically stressed that for data to be categorised as personal, a "content" element, a "purpose" element or a "result" element should be present; this clarification already provides for a relative interpretation.

Currently, it is almost impossible to ensure the full anonymisation of personal data and it is often possible to 're-identify' or 'de-anonymise' individuals hidden in anonymised data with astonishing ease[6]. We would also like to highlight that the US Federal Trade Commission has recently acknowledged the distinction between personally identifiable and non-personally identifiable data is no longer meaningful in light of developments in profiling technology[7].

BEUC urges the European Commission to reiterate the need for a broad and flexible definition of personal data in the forthcoming review. Given that the revised Framework will be in place for the years and decades to come, a restriction of the scope will be highly detrimental and will seriously jeopardise fundamental rights to privacy and data protection.

The issue that needs to be addressed is not the definition itself but rather the different interpretations and the subsequent lack of clarity at national level, as is the case for example with IP addresses[8] and energy consumption data from smart

---

4 Article 2.a Article 2.a of the Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

5 Article 29 Data Protection Working Party, Opinion 4/2007 of 20 June 2007 on the concept of personal data.

6 The question as to how the concept of anonymised data is subject to significant academic debate with several recent publications in the United States highlighting the ease with which anonymised data can be 'deanonymised'. De-anonymizing Social Networks, Narayanan and Shmatikov, Security and Privacy, 2009. Also Broken promised of privacy: responding to the surprising failure of anonymisation, Paul Ohm.

7 FTC staff report: Self-Regulatory Principles For Online Behavioural Advertising, February 2009.

8 Both the Article 29 Working Party and the European Data Protection Supervisor have taken the view that both static and dynamic IP addresses are personal data since a third party can easily discover the natural person using the IP address when even commonly available technology is used. According to the study commissioned by DG Markt on the relationship between copyright enforcement and data protection "IP addresses are generally considered by Data Protection Authorities and national courts to be personal; IP addresses are considered to be traffic data, which means that they may only be processed in a limited number of circumstances, for specific purposes and that consent is required to process them for other purposes, such as online copyright enforcement.

meters[9]. Clarification could be provided by the Article 29 Working Party within the framework of the enhanced role it should assume in the future.

2. Increasing transparency for data subjects

Introduction of a general transparency principle

BEUC supports the introduction of a general principle of transparent processing. Transparency has always been a key principle of data protection. Fair and lawful data processing requires that data subjects are sufficiently aware of what happens to their data so as to be able to exercise their rights.

However, the transparency requirements are not always met in practice. The many privacy policies of online service providers include complex and legal terms which fail to comply with the principles of transparency and fairness, aiming exclusively at complying with legal requirements rather than informing consumers. They are often obscure on issues where clear explanations matter the most, as for instance the question of whether data is shared with or sold to third parties, who these third parties are and what they intend to do with the data, the use of cookies and other data collecting technologies and data retention limits. Privacy policies are not always easy to spot on websites, while they may never be updated once they are published, even when the content and the nature of the service have evolved.

As a result, consumers rarely read and even more rarely understand privacy notices. This is confirmed by the figures provided by the Eurobarometer[10], according to which 64% of users feel that information on the processing of their data is not yet satisfactory. According to a study by the Norwegian Consumer Council, 73% of users aged 15-30 years seldom read Terms of Service[11], while the research carried out by Which? in March 2010 found that only 6% adults aged 16+ with internet access questioned have read the privacy policies of websites. These surveys demonstrate that although consumers are concerned about their privacy, they do not view the privacy policy as a suitable way to understand and answer their privacy concerns. These findings are confirmed by behavioural economics considerations, which show that consumers do not read privacy notices and are prone to accept default settings.

Lack of transparency and information is a major deterrent to users in the assertion of their rights. If they do not know how their data is being used, for what purpose and by whom, they will not be in a position to exercise and enforce their rights. The introduction of a general transparency principle will grant regulatory status and ensure its coherent implementation. **The information to the data subject should include further compulsory elements**, such as the competent data protection authority and its contact details, as well the modalities to access, rectify and delete their personal data.

In this respect, BEUC would support the development of **standard privacy notices** as a tool to enhance transparency and consumer control. This would require clarification and coherence of the legal framework, particularly as regards

---

9 Smart meters introduce the possibility of collecting detailed information on energy consumption usage and may raise privacy concerns, particularly when the data, resulting analysis and assumptions, are associated with individual consumers.

10 Eurobarometer survey on data protection in the EU - citizens' perceptions, February 2008;

11 http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf

definitions and modalities for exercise of rights, jurisdiction and applicable law. BEUC believes that Article 29 should take the lead in developing such standard privacy notices together with consumers' representatives and businesses.

However, increased transparency of privacy notices alone will not resolve all the current issues. It must be clear that posting policy notices on a website is not sufficient to conclude to have received informed consent from a consumer. The use of **Transparency Enhancing Technologies** (TETs), the development of notification standards by DPAs or even business could conduct focus groups and surveys to find out what the most efficient way to inform consumers is. The use of **layered privacy notices** i.e. first providing the user with a summary of key privacy points, and then providing access to the full privacy policy for those who wish to access more detailed information, should be further researched.

Specific obligations for processing of data related to children

Children and teenagers when surfing on the internet exchange a great amount of personal data through different means such as messages in chats and forums, photos and videos posted on social networks, blogs, profiles, geo-localisation, etc… This wide possibility to share data combined with the lack of awareness of the risks and dangers make children and teenagers the most vulnerable group in the digital world.

It is regrettable that the Communication only refers to children in the chapter on transparency. BEUC considers it is necessary to include specific provisions across the Directive, such as the obligation for data controllers to implement mechanisms for age verification, while data collectors should not collect personal information from children unless it is relevant, necessary and lawful[12]. In any case the collection and processing of children's sensitive data should be expressly prohibited. Public awareness campaigns targeted to children and their parents can provide an additional tool[13].

Horizontal data breach notification

BEUC welcomes the intention of the European Commission to explore the possibility of extending the mandatory personal data breach notification from the telecommunication sector to all relevant industries and sectors, including public authorities. In order for this requirement to be effective, it should only be limited to **serious data breaches** in line with a **proportionality test**, as notifying consumers about every data breach might distract their attention from serious data breaches. It should be for Data Protection Authorities to make such an assessment, in line with guidance to be provided at EU level.

---

12 Trans Atlantic Consumer Dialogue (TACD), "Children and electronic commerce", April 1999, Ref: DOC NO. ECOM-2-99;

13 For example, several NGOs (including the Bureau fédéral de la consommation BFC) have recently organised in Switzerland a campaign called "Stories from the internet… that no one wants to experience" about the risk of the internet addressed especially to parents and children: http://www.geschichtenausdeminternet.ch/index_en.html. Similarly, the campaign run by the Information and Privacy Commissioner of Ontario consisted of encouraging your people to consider that the "7 Ps" (Parents, Police, Predators, Professors, Prospective Employers, Peers and Pals) could view their postings online and to think about whether they were comfortable with the information they are sharing. A variety of channels to reach out to young people were used, including school programs, media, conferences, and partnerships with organizations that work closely with young people, as well as an innovative peer-to-peer network .

3. Enhancing control over one's own data

Principle of data minimisation

BEUC supports the strengthening of the principle of data minimisation. Although the current Directive has already established the principles of purpose limitation, minimum storage term and data quality, and therefore the principle of data minimisation is indirectly established, in practice it has not been complied with. For instance, profiling and data harvesting inherently require a service provider to collect large amounts of user data, often collected surreptitiously and stored for an unlimited period of time. Such setups obviously contrast with the data minimisation and transparency requirements laid down in the Data Protection Directive[14]. Similarly, ambient intelligence used for RFID applications and other sensors typically thrives in a data maximisation context, which can be difficult to reconcile with the principle of data minimisation. The explicit introduction would grant regulatory status and make it compulsory[15].

Provide for modalities for exercise of rights by data subjects

In order to ensure effective control over one's own personal data and the effective exercise of the data subject's rights, BEUC supports the introduction of specific modalities related to the right to access, correct and delete personal data.

Data controllers should not be able to charge for a data subject's access of their own personal data, as long as this right is not abused[16]. As regards the right to correct, erase and delete data, it should always remain free of charge, as it is also to the benefit of the data controller to have correct and updated data. Specific deadlines should be introduced for the data controller to comply with similar requests, depending on whether data are held within one environment, or within multiple, as is the case with banks and insurance companies. Furthermore, for the effective exercise of the right to access, correct and delete personal data, the development of an EU standard Subject Access Request Form should be considered.

Right to be forgotten

BEUC welcomes the intention of the Commission to introduce the right to be forgotten as a new right, particularly relevant in relation to social networks and cloud computing. Data subjects must be able to decide whether or not to share personal information as well as to impede the continue use of their data by data controllers, data processors or third parties. The right to be forgotten would enable the exercise of such a control.

---

14 EU study on Legal analysis of a Single Market for the Information Society the New rules for a new age? By DLA Piper – October 2009.

15 §3a of the German Federal Data Protection Act. has already introduced the principle that "data processing systems must strive to collect and process as few personal data as possible, and that (pseudo)anonymisation should be used when possible.

16 In those cases where data subjects have to bear a charge to get access to their data, there should at least not be any further increase until a clarification is provided at EU level.

The question that arises is related to the implementation of the said right. In France the issue has been debated within the frame of a draft law[17] which intends to implement the "droit à l'oubli numérique". In October 2010, several internet actors[18] signed together with the French government a Charter *« Droit à l'oubli dans les sites collaboratifs et les moteurs de recherche »*[19]. The Charter aims to improve transparency in the provision of information, improve the protection of minors online and facilitate the exercise of the "right to object". This represents an important step for the recognition of the right to be forgotten

The European Commission should build on the French experience and seek ways to ensure that the right to be forgotten can be effectively implemented; keeping in mind that it is crucial to ensure the fundamental right to freedom of expression is carefully safeguarded.

Right to data portability

Consumers are increasingly 'locked-in' to services provided by as well as to social network sites and it is not easy – if not impossible - to change from one service provider to another, due to all the messages/pictures/e-mails/videos one has stored.

Right to data portability should be understood as the right to recover and/or to shift from one platform/cloud to another material posted (e.g. photos). In our opinion, it is clear that consumers should **retain the ownership of data**. Existing terms and services appear mostly to be unfair and should be changed accordingly. Similar to consumers experiencing problems with DRM enabled specific operators digital content bundled with a specific software platform, the same will occur with personal data, when held in restrictive networks and platforms. However, for this right to be effective, **interoperability between services and promotion of open standards** is required.

4. Raising awareness

Awareness-raising campaigns can prove an effective tool in enhancing the understanding of data subjects regarding the challenges and improving their knowledge of their rights. However, for such campaigns to be effective, they should be organised by reliable organisations, including public authorities and national Data Protection Authorities. Civil society and consumer organisations have an important role to play as well. For instance, in April 2010 the German consumer association Verbraucherzentrale Bundesverband (VZBV) together with the German DPA organised a public awareness campaign with the aim of informing consumers about their rights vis-à-vis credit rating agencies; as a result, within three days more than 70,000 consumers exercised their right to access their personal data being stored.

---

17 Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure numérique, Novembre 2009.

18 The two major internet companies, Google and Facebook, did not subscribe the chart.

19 Secrétaire d'Etat chargée de la prospective et du développement numérique « Droit à l'oubli numérique dans les sites collaboratifs et les moteurs de recherche », 13/10/2010, available at: http://www.gouvernement.fr/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-proteger-les-donnees-personnelles-des-interna

5. Ensuring informed and free consent

Consent of the data subject is one of the possible criteria to legitimise data processing and therefore constitutes a fundamental element of the data protection legislation and an important tool of data subject's empowerment. What is critical to obtain is consumers' meaningful consent i.e. "free, informed and specific"[20]. However, not only has this concept been implemented differently by Member States[21], but in a number of cases, these conditions are not met raising serious concerns from the data subject's point of view.

First of all, consent cannot be given **freely** when there is a clear imbalance between the data subject and the data controller. For example, consent given for data processing by public authorities or within the context of an employment relationship fails to meet this criterion. Secondly, the need for consent to be **informed** is related to the failure to meet transparency requirements, as noted above.

In some cases, business models based on **profiling and behavioural advertising** may raise serious concerns as regards whether consent by online users complies with the requirements of the Data Protection Directive and the recently amended e-Privacy rules[22].

BEUC is concerned about the lack of transparency regarding the installation of **third party cookies** that are privacy invasive and allow for personal data to be sent to third parties, without the users' informed consent. Consumers are not even aware of what online behavioural advertising is. Research by Which? in the UK found that over 74% of over a thousand respondents had not heard of the term[23] and only 50% claimed to understand what cookies are[24]. These figures are confirmed by a recent scientific report, according to which 82% of young people are concerned that personal information is used without their knowledge, 75% that their identity is reconstructed using personal data from various sources and 69% that their views and behaviours may be misinterpreted based on their online behaviour[25].

As regards a **solution based on browser settings**, BEUC is concerned that it would put a disproportionate burden on users to protect themselves. Currently, the vast majority of browsers are set to accept third party cookies as default, and users

---

20 Article 2 (h) and Article 7 of the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

21 Several laws emphasise the need for any consent to be manifestly free, specific and informed etc., by including the term "unambiguous" in the very definition of consent (Portugal, Spain, Sweden); the Luxembourg law even includes both the term "unambiguous" and the term "explicit" in the definition. The laws in Germany and Italy stipulate that consent should (in principle) be in writing (while allowing for the giving of consent on the Internet by means of a "mouse-click"). By contrast, guidance on the law, issued by the UK data protection authority, suggests that consent for the processing of non-sensitive data can often be implied. *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Centre for Public Reform, 20 January 2010.*

22 Article 5.3 of the revised Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

23 General public face-to-face omnibus survey, October 2010. Base: 1, 042 adults.

24 General public face-to-face omnibus survey, February 2010. Base: 1, 468 adults with internet access.

25 Scientific report 'Young People and Emerging Digital Services', 2009: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu

must themselves change the privacy settings of their browsers. However, it is highly unlikely that the average user, who lacks both the necessary information about behavioural advertising and the technical knowledge to change his browser settings, will ever take such action. Therefore, it would be wrong to presume that users have provided their implicit consent by not changing their browser settings. Furthermore, currently browser settings are not flexible enough to allow for consumers' choices as regards the cookies they may want to accept or reject.

In addition, the consumer's choice to reject third party cookies may be circumvented by so-called '**flash cookies'**. Flash cookies are problematic as they are stored in a different location than regular http cookies and are not removed if you delete cookies from within your browser. Even the 'Private Browsing' mode recently added to most browsers does not stop 'flash cookies' from operating fully and tracking consumers[26].

Lastly, a browser-based solution would not be appropriate when considering that consumers move **towards an increasingly application-centric environment** which is often accessed via mobile devices.

If browser settings are to be promoted as the solution, BEUC firmly recommends that specific actions are needed to ensure browsers are redesigned in compliance with the **privacy and security by default principle.** The problem of low consumer awareness of cookies needs to be addressed while ensuring that consumer choice is respected. The recent proposal of the US Federal Trade Commission suggesting the implementation of a '**Do Not Track'** setting on consumers' browsers, is worth exploring[27]. In any case, consumers should be able to easily activate a 'do please track' setting to access full functionality of a given site if they wish to do so.

It must also be recognised that **cookies are no longer the only way to track users online**[28]. The list is ever expanding as industry innovates to collect more and more data, at an increasingly granular level.

BEUC recognises that **there is no 'one size fits all'** solution to the issue of consent, while the means of implementation of consent of consumers should be flexible and user-friendly. We believe that practices could be assessed against the two following criteria:

1. An analysis of the potential consumer detriment linked to a specific practice/ technique.
2. An evaluation of whether a practice/technique meets the 'reasonable expectations' of uses of their information by an average or typical consumer or by the average member of the group when it is directed to a particular group of consumers.

Given the importance of the issue of consent, we welcome the intention of the European Commission to clarify the rules on consent involving in the discussion all stakeholders concerned, while ensuring greater harmonisation at EU level.

---

26 UC Berkeley research study on flash cookies http://www.law.berkeley.edu/institutes/bclt/about/about_news_08-17-09_3.htm

27 http://www.ftc.gov/opa/2010/12/privacyreport.shtm

28 JavaScript is being utilised to read which websites have been visited previously, and serverside computer identification which has come to light with the recent EFF Panopticlick, would all be examples of new tracking technologies.

6. Protecting sensitive data

Although the text of article 8(1) of the 1995 Data Protection Directive is still valid, it does not reflect the recent technological developments which increase the risk of using data that a priori might not be considered sensitive for discriminatory proposes. BEUC has identified the following categories of personal data that should be classified as sensitive data as well:

- **Biometric data**: given the special characteristics of biometric data, in that it may be related to health and genetics and also that it is a sort of 'universal key' in getting all kinds of personal information, it should be considered as sensitive personal data[29].
- **Family history**: the collection and processing of data related to family antecedents could easily reveal the ethnic origin of a person.
- **Minors' data:** due to their emotional situation and the lack of critical judgement, minors do not take steps to protect themselves, despite the fact that they may acknowledge the risks to their privacy[30].
- **Data of financial nature:** the collection and processing of financial data, when revealing personal solvency, should be considered as sensitive. A survey carried out in 2006 by the Office of the Information Commissioner in the UK revealed that 70.5% of respondents considered financial data as extremely sensitive. Other financial data such as the unpaid debts of clients to the company with which it is or has been in a contractual relationship would not make part of this category.

BEUC believes that the new Framework should provide for a **non-exhaustive list of sensitive personal** data, thus allowing for flexibility in light of new technological developments.

7. Making remedies more effective

Efficient redress is a key component of a data subject's empowerment. Although the current Directive already foresees the possibility for individuals to seek redress and compensation for damages suffered as a result of a data breach, in practice this provision has not been implemented effectively. The high costs related to individual litigation, as well as the legal uncertainty as regards competent forum and applicable law act as a deterrent in the enforcement of data subject's rights and an impediment to the fundamental right of access to justice.

In addition, when it comes to data breaches, the damages suffered are typically too small on an individual scale and would entail significant and disproportionate costs; however, the collective damage is significantly more substantial. An illegal behaviour of abuse of personal data can easily affect a high number of people, especially in the online environment, where online services are cross-border and often provided from outside the EU. Furthermore, damages suffered are often intangible and it is difficult to assign a value and determine the responsibility of the

[29] Arguments and evidence in Identifying Legal Concerns in the Biometric Context, by Yue Liu, Norwegian Research Centre for Computers and Law, University of Oslo, published in Journal of International Commercial Law and Technology Vol. 3, Issue 1 (2008).

[30] According to the Scientific report 'Young People and Emerging Digital Services', 2009, 82% of young people are very concerned that personal information is used without their knowledge http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119.

involved parties, while in some cases, there might be no immediate damages, such as when confidential data (credit card numbers) are leaked.

BEUC and its members have long been advocating for the establishment of a **judicial collective redress mechanism**, both at national and European level, and have taken a firm position on the elements of such a mechanism based on evidence, research and scientific data[31]. Nevertheless, the European Commission has been reluctant to adopt a binding EU instrument establishing judicial collective redress. We would like to reiterate our support for such a mechanism as an efficient tool for consumer empowerment and business compliance.

8. Applicable law and jurisdiction

We welcome the fact that the Commission intends to address the issue of the applicable law in order to put an end to the existing legal uncertainty surrounding it. Indeed, many companies established outside the EU claim that they are not subject to European law, but to their national law.

When dealing with the issue of applicable law, it is essential to keep in mind that the main aim of the Directive is to protect the rights of the data subjects[32]. In practice, when there is an element or factor closely connected to the EU, which helps protect the interests of EU citizens, the legislator[33] and the judge[34] often decide in favour of EU law.

BEUC believes that **EU law should apply to cases where services are targeted at EU citizens in line with the criteria established by Article 29 Data Protection Working Party[35]**. More specifically, the law of the data subject's country of residence should apply. In other cases, EU law would be applicable in the conditions described by the Article 29.

9. Joint responsibility between data controller and data processor

We urge the European Commission to consider and clarify the responsibilities of those involved in data processing, as in practice the chain of responsibility and liability is getting difficult to follow for data subjects as the relations between data controllers and data processors are increasingly complex (e.g. cloud computing). In practice, the distinction between data controller(s), data processor(s) and third parties is blurred.

---

31 For further information, see BEUC 10 Golden Rules on group action, as well as BEUC's response to the Green Paper on consumer collective redress X/016/2009 – 09/03/09.

32 This is confirmed by recital 20 of the directive on data protection which states that *the fact that the processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive".*

33 See article 12 of the Distance Selling Directive (Directive 97/7/EC), Article 6(2) of Directive 93/13 on Unfair Terms in Consumer Contracts and Article 7(2) of Directive 99/44 on certain aspects of the sale of consumer goods and associated guarantees and article 6 of the Rome I Regulation (Regulation 593/2008/EC).

34 See ECJ jurisprudence on the Rome Convention; e.g. Ingmar GB Ltd. and Eaton Leonard Technologies Case C-381/98.

35 Opinion 8/2010 on applicable law, adopted on 16 December 2010.

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu

All actors should have a share of responsibility to ensure that the data being circulated, collected and processed is secured. If consumers want to exercise their rights, they will turn to the business they have been in contact with; in the online world, it would typically be the website portal. Thus, if a consumer asks the business they were in contact with to rectify or delete their data, the business should also notify this fact to third parties to whom personal data had been disclosed. Similarly, if information is misused by third parties that are hosted by a service provider and there is a breach of privacy, then liability should rest with the service provider.

Therefore, we would urge the European Commission **to set up joint and several liability rules between a business and third parties in case of breach**, in order for the consumer to be able to claim full compensation for the damage suffered from any of them[36].

10. Privacy by design

BEUC is concerned that the Communication does not fully recognise the importance to technological solutions as a tool to enhance control by data subjects, by simply considering them an internal market issue. On the contrary, we firmly believe that technical means and technological solutions can help to empower data subject's control and enhance the enforcement of the data protection legislation.

BEUC urges the European Commission to **include privacy by design as an explicit, mandatory principle** in the new Framework for Data Protection. Privacy and security by design should require privacy and security to be embedded in ICT technologies during the whole life cycle, from the design of specifications of systems and technologies. This would make its implementation compulsory by both ICT manufacturers and data controllers, while providing for its effective enforcement by Data Protection Authorities. BEUC firmly believes that this principle should be **technology neutral** to apply across the sectors, from transport and health systems to social networks and ICT devices. The principle could be further specified in sector-specific legislation. Such technical solutions should comply with the principles of data minimisation, transparency, data confidentiality, purpose limitation, data security and foster consumer empowerment.

Any technical solution should comply with the principle of data minimisation, data security and foster consumer empowerment. A good example is **Privacy Enhancing Technologies** (PETs). PETs could help limit the collection of personal data and serve as identity management instruments. When developed, PETs should apply the PRIME principles such as e.g. design must start from maximum privacy[37].

---

[36] For instance, in Denmark a sector agreement has established a joint-liability between the mobile phone companies or Internet Service Providers and third parties such as mobile content providers. The mobile company takes the responsibility for the services provided by third parties and in return gets a percentage of the revenues generated by the services (e.g. on ring tones, virtual websites sale, Facebook applications etc.).

[37] PRIME (privacy identity management) project - This includes design must start from maximum privacy; explicit privacy governs system usage; privacy rules must be enforced, not just stated; privacy enforcement must be trustworthy; users need easy and intuitive abstractions of privacy; privacy needs an integrated approach; and, privacy must be integrated with applications https://www.prime-project.eu/about/principles/

The risks need to be minimised on a technical level by building in privacy and security protection and on an operational level, by prescribing and enforcing privacy standards.

II. Enhancing the Internal Market dimension

1. Increasing legal certainty through further harmonisation

We share the opinion of the European Commission that further harmonisation of the data protection legislation may be necessary to provide both data controller and data subjects with more legal certainty, particularly in the current context of cross-border flow of personal data.

However, further 'approximation' of national laws should take place at a level that would at least clearly meet the requirements of the most demanding constitutions and the nature of data protection as fundamental right. Further harmonisation should not result in reducing the level of protection for data subjects.

We are concerned the European Commission may opt for the adoption of a Regulation as the legal instrument; this would open up complex questions of subsidiarity and legal competence and would make the resulting rules less flexible, while it may compromise the legislation of those Member States where data subjects enjoy a high level of protection.

It is therefore crucial that before any proposal is adopted, a very careful assessment of the possible impact on national legislation and the rights of data subjects is carried out, as well as a consideration of the effectiveness of different legal instruments. The role of the Article 29 Working Group could also be strengthened with the aim of using its expertise and the direct link with national practices to provide for harmonised interpretations of key issues and ensure a coherent application of the provisions of the Directive.

2. Reducing the administrative burden

The reduction of unnecessary administrative burdens would be an efficient way to bring more coherence and facilitate the free flow of personal data. BEUC agrees with the analysis of the European Commission that the current system of notification should be simplified, as long as the new Framework results in more coherent rules across Europe.

Considering the significant divergence in national rules regarding notification[38], BEUC welcomes the **development of a uniform notification model** which would help to remove the current complexities and administrative burden from both DPAs and businesses.

[38] EU study on Legal analysis of a Single Market for the Information Society the New rules for a new age? By DLA Piper – October 2009.

However, **BEUC is opposed to the abolition of the notification procedure**, as it provides an important tool for DPAs when considering enforcement, while if done properly, can enhance transparency for data subjects.

3. Enhance data controller's responsibility

Accountability principle

BEUC supports the **introduction of an explicit accountability principle**, according to which the data controller and, where appropriate, the data processor, will have to take appropriate measures to ensure and demonstrate compliance with the data protection legislation.

To this end the mandatory carrying out of **Privacy Impact Assessments (PIAs) and audits/controls** could indeed enhance the responsibility of data controllers. However, for such measures to be effective, they need to be regularly verified and certified by independent parties and should not be considered as substitutes to compliance with data protection legislation and enforcement.

In addition, the compulsory appointment of a **Data Protection Officer (DPO)** in companies collecting and/or processing personal data as is already the case in Germany, should be considered. Nevertheless, this would require the establishment of clear criteria for the certification of the qualification of DPOs and their expertise. According to the Eurobarometer (2008) survey[39], only 13 % of people responsible for data protection within companies said they were very familiar with the provisions of the data protection law.

4. Encourage self-regulatory initiatives and explore EU certification schemes

Self-regulation

BEUC is concerned about the intention of the European Commission to encourage the development of self-regulation in the field of data protection. Self regulation proposals can only be accepted if they entail an **added value for consumers' rights by offering more extended rights, fully compliance with the existing legislation, implementation by the whole industry, provision for independent complaint handling and enforcement mechanisms and are approved by an independent authority.**

Nevertheless, recent proposals for self-regulation by the European Advertising Standards Alliance in the field of online behavioural advertising[40] are far from complying with these principles. In particular, BEUC has serious concerns with this system for a number of reasons:

- First of all, it is **questionable whether an icon-based system can actually enhance consumers' empowerment**. A recent TRUSTe study in the US with a comparable logo, showed that out of approximately 20 million consumers (7

[39] Eurobarometer survey on data protection in the EU, February 2008.
[40] http://www.easa-alliance.org/Issues/OBA/page.aspx/386 ;

million unique visitors), it was accessed 56,000 times with 44,000 unique views. If calculations are just made on the unique visitors and unique views, this means that only 0.6% of consumers clicked through to the ad info page. This, in no way, signifies informed consent.

- Secondly, even if consumers click on the icon they will be taken to another webpage where they will only find information regarding the **positive aspects of behavioural advertising** and a multitude of links to other web-pages.
- Thirdly, **consumer redress, enforcement and sanctions** will be handled by industry bodies, rather than independent authorities, while there are specific deadlines for handling consumers' complaints;
- Fourthly, it is highly questionable **whether all industry players** will adhere to such self-regulation. The recent example in the UK, where the Code of Conduct by IAB is only applied by 8 out of the 540 members is clear example of the low take-up.

Another example refers to the "Safer Social Networking Principles for the EU[41]". The European Data Protection Supervisor has recently outlined a number of areas where no action has been taken, such as communication of safety measures and tools available on the web portals of social networks and the restriction of access to the profiles of minors only to their friends[42].

EU certification schemes

In line with our call for the explicit introduction of the 'privacy by design' principle in the new framework, the development of **EU certification schemes and privacy seals** could become effective means to ensure 'privacy compliant' or even 'privacy enhancing' IT products and services. It will also provide an incentive for developers and providers of such products and services to invest in better privacy protection, while allowing users to make an informed choice.

BEUC would support the establishment of EU certification schemes, including European Privacy Seals, as long as clear certification criteria are developed and the administration is entrusted to independent third party organisations. For instance, the success of the EuroPriSe scheme[43] is linked to the fact that the criteria applied are very strict and set by data protection authorities in countries with strong data protection. The establishment of a Certification Authority for the issuing of the seals and the accreditation of specially trained and tested independent experts, who carry out the primary evaluation of the products provide for additional safeguards.

We would also like to encourage the European Commission to include a specific obligation for public authorities in the Member States and EU bodies to procure privacy-compliant products and services whenever possible[44].

---

41 The principles are available at: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

42 Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (2010/C 280/01).

43 https://www.european-privacy-seal.eu/ .

44 An attempt has been made to address this in the data protection law of the German Land of Schleswig-Holstein https://www.datenschutzzentrum.de/guetesiegel/index.htm .

III. Revising the data protection rules in the area of police and judicial cooperation in criminal matters

N/A

IV. The global dimension of data protection

Rules for international data transfers

As more and more processing operations take place in a global context, it is important to adapt the EU framework with the aim of ensuring the free flow of data, while guaranteeing the level of protection for data subjects' rights. In particular, the criteria for the **adequacy procedure** need to be clarified and further strengthened, while the procedure for the analysis of the legal regimes of third countries need to be streamlined and improved with the aim of also considering the actual implementation and enforcement of the rules in those countries.

As regards the conclusion of **international agreements** between the EU and third countries, BEUC firmly believes that such agreements should reflect the high level of protection of personal data in the EU and provide for effective compliance and enforcement mechanisms. For instance, the **Safe Harbor Agreement** between the EU and the US has failed to be effective, because of the minimum possible requirements of the agreement and the considerable differences of legal traditions between the US and the EU[45], while its enforcement has proven problematic[46].

Promoting universal principles

BEUC believes that the development of universal principles and global standards is necessary, in light of the cross-border flow of personal data. The International Standards on the Protection of Personal Data and Privacy – the so-called '**Madrid Declaration**[47]' that were recently adopted and supported by both civil society and private corporations constitute a first step towards the development of a set of binding international privacy principles. The EU should also continue to work with international organisations to achieve this goal. For instance, the forthcoming revision of the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 2011 is an opportunity for the EU to ensure greater convergence with the new EU Framework.

---

45 EuObserver.com, EU privacy rules changing US companies available at: http://euobserver.com/9/30372

46 In its 10 years of existence, Safe Harbour has seen only seven cases brought to court in the US - all were companies wrongly stating they were part of the scheme, not actual non-compliance cases. None were notified to EU data protection authorities.

47 Joint proposal for a draft of international standards on the protection of personal data and privacy, agreed at the 30th International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009.

In addition, the development of **international standards** has the potential to ensure a coherent and effective implementation of the data protection regulatory requirements. Such standards will be of particular importance as regards the technical modalities of access to personal data, the implementation of the privacy by design principle and the development of standard privacy policies. However, in order to be effective, they need to be developed within the standardisation organisations. For instance, the European Committee for Standardisation (CEN) has created a Workshop on Data Protection and Privacy (DPP), which contributes to resolving ICT technical compliance issues, taking into account EU data protection legislation[48].

V. Stronger institutional arrangement for better enforcement of data protection rules

Role of Data Protection Authorities

BEUC recognises that Data Protection Authorities have an important role to play, both in ensuring compliance with the legal framework and in enforcement. However, a number of shortcomings have so far prevented them from fulfilling their mission, including a lack of independence, adequate resources and sufficient powers.

As the challenges to data protection increase, particularly in light of technological developments, the new framework should guarantee uniform standards as to their independence, both institutional and material of DPAs. They should be provided with the means to develop technical competence to understand the privacy implications of the new technologies, to control and impose sanctions. In 2008, the German Federation of Consumer Organisations (VZBV) was able to buy six million sets of consumer data on the black market for €850. The seller of this data was only punished with a fine of €900. The sanctions DPAs can impose need to have a clear deterrent effect.

Additional measures to improve the cooperation and coordination between national DPAs are also necessary, given the cross-border flow of data and the need for more cross-border enforcement.

Article 29 Working Party

BEUC recognises the importance of the work carried out by Article 29 Working Party and strongly believes that its role and missions should be strengthened in the new data protection Framework. First of all, we would advocate that its Opinions should become binding on the European Commission and should be reflected in the Commission's proposals. Secondly, its opinions should be put into guidelines by national DPAs for better consistency across the EU. Interpretative communications from the European Commission on some particular provisions of the Directive would also be helpful. In addition, the Article 29 Working Party has a role to play in clarifying specific notions of the data protection legislation, such as that of 'consent' and should be involved in developing privacy standards and assessing the

[48] www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/wsdpp.asp.

implementation of the 'privacy by design' principle for new technologies and business models.

Role of consumer protection authorities

In addition, one should reflect on the role consumer protection authorities could play as additional enforcers. In fact, poor data protection or privacy practices often come in the shape of unfair contractual terms or unfair commercial practices. The role of 'traditional' consumer protection law as a means to protect consumers' data protection and privacy should be investigated further.

END

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu