

A vertical bar on the left side of the page consists of 20 small, colorful icons of shopping carts. Each icon is set against a different colored square background (purple, red, blue, orange, pink, yellow, green, etc.) and is oriented diagonally.

EU GENERAL DATA PROTECTION FRAMEWORK

BEUC answer to the consultation

Contact: Emilie Barrau and Nuria Rodriguez –

digital@beuc.eu

Ref.: X/106/2009 – 31/12/2009

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

Summary

BEUC very much welcomes this timely consultation. We fundamentally believe that the existing core principles of the data protection Directive remain relevant and must be retained. It is equally important that the Directive stays technology neutral. We are also convinced that many aspects of the Directive have not been explored to their full potential – let alone the poor level of compliance and enforcement.

We have identified several challenges and risks linked to the use of personal data in the digital world. The following initiatives would allow the Directive to be more effective in protecting consumers' data and privacy:

- **Improve the enforcement of the Directive could be achieved:**
 - **Through technical solutions:** Article 17 of the Directive should be interpreted to give legal foundation to "privacy by default";
 - **By business players:** compulsory Privacy Impact Assessments and audits/controls, prior testing, staff training and data protection officers should be put in place;
 - **By Data Protection Authorities (DPAs)/consumer authorities:** DPAs must be given the means and the tools to fulfil their mission. The role of "traditional" consumer protection authorities should be investigated further and eventually reviewed.
 - **By data subjects:** they should give meaningful consent to the collection of their data. Online, consumers should have the possibility to exercise their rights freely and via electronic means. Consumers should be compensated for any detriment they may suffer as a result of data breaches or unauthorised use of data. While there is a role for better information and education of consumers, we cannot put the full responsibility on consumers' shoulders.
- **Ensure Fairness and Transparency:**
 - Fairness of terms needs to be improved and policy notices need to be clearly displayed in plain and intelligible language. Notice must be provided at the "point" of collection.
- **More Accountability:**
 - A strong sense of public accountability needs to be developed amongst data controllers and data processors;
 - Horizontal rules concerning the prevention, management and reporting of data breaches are needed;
 - Joint and several liability rules between a business and third parties in case of breach should be set up, in order for the consumer to be able to claim full compensation for the damage suffered from any of them.
- **Clarification and harmonisation of rules:**
 - The questions of national implementations of the Directive and interpretation of its key concepts need to be addressed;
 - BEUC believes that EU law should apply to cases where services are targeted at EU citizens. In case of litigation, the competent court should be that of the country of residence of the data subject.

In addition, we believe that **new rights** specific to the Digital Age such as the **right to be "forgotten"** and the **right to data portability** should be introduced in a new instrument.

PART I – ISSUES AND CHALLENGES

I. Introduction

The data protection Directive 45/96/EC (hereafter “the Directive”) constitutes the fundamental legal framework governing the processing of personal data in the EU. The transparency of data collection, fair and lawful processing, purpose limitation and specification, data minimisation, consent, right to access, object, correct and withdraw one’s data, are among the core principles consecrated in this text.

Yet, during the 13 years since the Directive was adopted, far reaching changes have occurred in the way personal data is accessed, processed and used, particularly as a consequence of the advent of the Internet and online communications.

While we acknowledge the numerous problems that exist in the offline world, the aim of this position paper is to assess the extent to which the principles in the Directive are still valid in the context of the new information and communications technology, as well as to put forward a number of proposals to solve new challenges and/or gaps as regards the protection of personal data in the digital environment.

In order to do so, it is important to keep in mind the wide scope of the definition of personal data (as supported by article 29 Working Party¹) as a term that encompasses any information that may be linked to an individual. This is relevant, especially regarding the profiling and targeting practices of some web companies. **BEUC fully supports a wide definition of personal data as provided in the opinion of article 29 working party.**

Moreover, the scope of the definition of “processing” is sufficiently large to encompass almost any operation in the online world that involves personal data. This interpretation has also been endorsed by the European Court of Justice (ECJ) in the Lindqvist case law².

II. New challenges and risks in the digital environment

Since the adoption of the Directive, the rapid development of the information and communications technology together with the development of new services applying ever changing business models, raise a number of challenges as to the

¹ Article 29 Data Protection Working Party, Opinion 4/2007 of 20 June 2007 on the concept of personal data (WP 136):

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

² ECJ Case C-101/01 of 6 November 2003; The Court held that “The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.

practical application of the principles of the Directive to the online environment. Today, one person in two in the EU27 uses the Internet daily³.

As we know, the online environment results in new and unprecedented risks to privacy which cannot be compared to those occurring offline. However, **a consumer's right to privacy should not be undermined or mitigated merely because it has become easier and more profitable to break it in the virtual world**. In order to protect and develop consumer confidence in new digital markets, BEUC believes that it is critical that general principles regarding privacy and contract law are enforced also in the online environment.

In the online environment, consumers are frequently required to give away their data at different levels (e.g. Internet Service Providers, web browsers, social networks platforms, search engines...). The majority of current practices of Internet companies do not respect the data protection Directive requirements and thus are a source of continued consumer detriment and lack of confidence when it comes to the online protection of personal data⁴. Below we identify some of these problematic areas while in part II of this paper we put forward proposals on how to address the new challenges of the online world while ensuring a high level of consumer protection in this field⁵.

❖ Lack of transparency

Articles 10 and 11 of the Directive consecrate the principle of transparency of data processing. Data controllers (or data processors) are obliged to inform data subjects about the collection and processing of personal data and to provide certain information to the data subjects.

Yet, **many privacy policies of online service providers do not abide by the compulsory transparency requirements**. The vast majority of consumers do not currently read privacy notices due to their length, complexity and complicated language⁶. The notices fulfil legal business obligations rather than informing consumers. They are often obscure on issues where clear explanations matter the most (for instance on 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 a website. Moreover, some privacy policies are never updated once they are published, even when the content and the nature of the service have evolved.

The lack of transparency about the use of the personal data across the Internet is an obvious deterrent for users in the assertion of their rights. Who is ultimately responsible for data collection and retention and where to seek redress is often left unclear. It follows that if consumers do not know how their data is being used, nor

³ Eurostat, Data in Focus 46/2009 "Internet usage in 2009 - Households and individuals"

⁴ In a study published by the Consumer Council of Norway in November 2009, 94% of consumers asked say that it important to retain control of their personal information that they share online. 67% of the same respondents are worried over the consequences of sharing personal information online. See:

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

⁵ Recital 10 of the Directive.

⁶ A study produced by the Consumer Council of Norway documents that consumers generally do not understand the terms of service that is offered by their favourite social networks, <http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf>

who it is being held by, they do not know what questions to ask, nor who to direct these questions to.

We therefore come to the conclusion that **transparency and consumer friendly access routes to the data controller are of paramount importance in the online environment.**

❖ **Lack of a meaningful user consent**

While it is important to note that there are several ways to validate the processing of personal data, the requirement to obtain **users' consent**, wherever relevant, **is frequently infringed in the online environment.** Very often personal data are collected and processed without informing and obtaining the data subject "free, informed and specific" agreement about such collection and processing⁷.

Most data controllers claim to meet the consent obligation through the publication of their privacy policies. However, as pointed out above, most privacy policies do not allow consumers to give a **meaningful consent**⁸.

Aside from the privacy sensitive features of profiling and targeting business models, other business models, relatively new, are emerging and need to be looked at. For instance, we would like to draw the attention to the lack of legal certainty that surrounds **unsolicited data aggregation websites.** These websites are based on collection, processing and aggregation of data available on the Internet without any intervention of the data subject and thus without requiring his/her consent.

❖ **Illegitimate processing of personal data**

Following article 6 of the Directive, personal data can only be processed in a fair and lawful way and for specified, explicit and legitimate purposes. Processing cannot thus take place beyond those purposes.

This legal requirement seems to be contradicted by some of the business models currently adopted on the Internet. **The business models of many Internet companies (e.g. some search engines, social networking sites...) are not always compatible with the principle of purpose limitation and the specification of use of personal data.** For instance, many companies collecting personal data transmit the data to third parties that often process these data for different purposes from those initially pursued by the data controller⁹.

⁷ In the Consumer Council of Norway study, 58% of consumers asked think they have lost all control over how their personal information is being used by commercial parties online, see <http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf>

⁸ The abovementioned Norwegian study reveals that 73% of users aged 15-30 rarely or never read the terms of service (TOS). Only 4% of these users claim to read terms of services routinely. During the study, a selection of TOS were put under evaluation and measured against some key consumer expectations, for a general overview of the results, see http://forbrukerportalen.no/filearchive/matrix_terms.jpg

⁹ For instance, about 350 000 third party applications are offered through Facebook. By default, Facebook user information is shared with these third parties.

❖ **Processing of personal data for an excessive period of time**

The Directive (article 6.1) allows personal data to be kept by companies only for the time strictly necessary for the purposes for which it had been collected.

Even though we acknowledge adherence to the limitation criteria is difficult to assess and may depend on the specific case, **many data controllers retain data beyond the necessary time to perform the service.**

In the specific case of search engines, the article 29 Working Party requires search engine providers *"to delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times"*¹⁰. The Working Party does not see a basis for a retention period of personal data by search engines beyond 6 months. However, many cookies are set up to "live" forever and search engines keep data over 6 months e.g. Google (9 months for IP addresses and 18 months for cookies) and Yahoo! France (13 months for IP addresses and 2 years for cookies).

❖ **Difficulties to access, correct and withdraw one's personal data**

The Directive (article 12) establishes the right of the data subject to have access to his/her personal data processed by the controller and to correct and/or delete the data, particularly if processing does not comply with the legal requirements or goes beyond the legitimate purposes surrounding the collection and processing.

The rights of data subjects to access, object or erase their personal data are not always acknowledged by online service providers. Various studies and surveys have reported the difficulties data subjects have in exercising such rights.

For instance, UFC Que choisir has recently published the results of a survey which demonstrates that the majority of companies operating on the Internet are very reluctant to reveal, correct or withdraw the personal data they retain¹¹. Similarly, the study of the Consumer Council of Norway demonstrates that users of social networks generally have little or no opportunity to exercise their right to correct or withdraw their data once they have been shared with third parties¹².

Some companies¹³ even claim that they own or have a perpetual licence to use the content uploaded by the consumer to their website. This assertion is often hidden deep within the website's terms and conditions and is rarely noticed by the average consumer.

¹⁰ Article 29 Working Party opinion 1/2008 on search engines (April 2008).

¹¹ Companies such as Free, Air France, Bouygues Telecom refused to give access to personal data. Other such as Champion, La Redoute, Le Monde ou Medecin sans frontiers refused to withdraw personal data from their files. UFC 29/10/2009.

¹² See study at:

<http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf>. On basis of this study, the Consumer Council announced that they will file a complaint against Facebook and other social media to the Norwegian Data Inspectorate.

¹³ For instance LinkedIn and Twitter; see:

http://forbrukerportalen.no/filearchive/matrix_terms.jpg

❖ **Lack of liability of third parties**

The party responsible for ensuring that data protection principles are complied with is the data controller (article 6.2), who determines the purposes for which, and the manner in which personal information is to be processed. In certain cases, the data controller delegates this task to a data processor in which case the latter bears the responsibility for the handling of the data. The data controller can also allow third parties to access the data.

Yet, as a matter of fact 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).

Often third party applications that can be added to a service or platform are regulated by terms other than the host's website – or sometimes no terms at all – , even though the consumer might believe these are "approved" by the data controller as they seem to be a part of the site. Third party applications often fail to be transparent about the fact that they harvest both the users' and their contacts personal data from their social networking sites.

In practice, the distinction between data controller(s), data processor(s) and third parties is blurred. **Currently there is a total lack of transparency as regards the various parties involved and their responsibilities.**

❖ **Lack of proper enforcement of the data protection Directive**

The EU owns a strong regulatory framework that theoretically protects the interests of individuals when it comes to the collection and processing of their personal data. However, in practice few companies abide by the existing rules, particularly in the realm of the Internet.

Proper surveillance of the market and enforcement of the legislation is almost non-existent and companies continually get away with infringements of the existing laws – both offline and online. Already, at the time of the first Commission Report on the implementation of the Directive, reference was made to the *"under-resourced enforcement effort"* and the fact of dealing with *"supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority"*¹⁴.

While we acknowledge that the complexity of the Internet ecosystem -involving the processing of enormous amounts of data by different actors in a borderless environment - represents a substantial challenge, appropriate solutions need to be urgently found to achieve better compliance levels with the data protection regulatory framework.

❖ **Legal uncertainty regarding the applicable law and the competent jurisdiction**

One of the most difficult issues when trying to reconcile the data protection Directive with the realities of the Internet is that of deciding which law should be

¹⁴ First implementation report of the European Commission on the Data Protection Directive, 15 May 2003:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT>

applicable to the collection and processing of personal data, particularly when the data controller is established outside the EU.

Article 4 of the Directive states that EU law is applicable when the data controller has an establishment in one of the EU Member States or when a controller, established outside an EU Member State, makes use of any “equipment” situated in the territory of a Member State.

Yet, the application of this rule is rather controversial¹⁵ and the divergences in national implementations further complicate its application in particular when it comes to cross-border cases¹⁶.

As a matter of fact, **currently many companies based outside the EU** – like Google or Facebook for instance – **still claim they are not subject to European law but to their national law**¹⁷.

III. Examples of privacy-sensitive Internet services and applications

❖ Search engines

BEUC acknowledges the crucial role of search engines in the information society as intermediary facilitators of information. Yet, protecting users’ privacy and guaranteeing their rights, such as the right of access to their data, providing transparent privacy policies and business models, are all sensitive issues surrounding the business models of many search engines¹⁸.

The aggregation abilities of search engines through combined search queries and their storage can significantly reveal individuals’ personal characteristics and behaviours. These practices have a strong impact on the right to privacy¹⁹, even more if the personal data in the search results are incorrect, incomplete or excessive²⁰.

¹⁵ See Article 29 Working Party’s working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30 May 2002:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

¹⁶ For instance the interpretation of the concept of “establishment” differs among members states (see “European Study on the Legal Analysis of the Single Market for the Information Society”, by DLA Piper for the European Commission)

¹⁷ For instance Facebook, LinkedIn, Twitter, Google and Bing apply US law.
http://forbrukerportalen.no/filearchive/matrix_terms.jpg

¹⁸ Resolution on Privacy Protection and Search Engines, adopted by the 28th International Data Protection and Privacy Commissioners' Conference.

¹⁹ International Working Group on Data Protection in Telecommunications:
<http://www.privacy.org.nz/international-working-group-on-data-protection-in-telecommunications-iwgdp/>

²⁰ In the summer of 2006, a service provider published a sample of queries and results of some 650.000 users during a 3 months period. Even though AOL had replaced the names of the users by a number, journalists found out these results could often be traced to individual users, not only because of so-called ‘vanity searches’ (people searching for information about themselves) but also by combining several queries by a single user. See the article 29 working party opinion on search engines of 4 April 2008:

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

Most often consumers are unaware of such practices as they are not properly informed about what is going on “behind the scenes” and thus cannot evaluate the sensitivity of the information contained in search logs.

The deletion of “cookies” that allow such profiling is not made easy: the ‘opt-out’ cookie gets deleted each time the user uses the browser options to delete cookies; changing privacy settings within browsers is often complicated and little advertised and certain cookies (flash cookies) simply cannot be erased.

❖ **Social networks**

Social network services have become very popular in recent years²¹. Facebook, LinkedIn, mySpace etc provide a range of services such as blogging, posting, forum discussions, instant messaging, photo publishing etc.

Even though privacy settings allow users to take action to restrict the circle of people to which they give access to their data and content, it is often complicated and burdensome; some social network sites have been criticised for enticing and encouraging members to open their network as much as possible – as default settings are set to have the data available to everyone²².

Many social networks perform data mining operations on the data uploaded by their users. Their business model is based on the secondary use of data gathered from their members, mainly for marketing purposes. This model entails that **personal data are processed for purposes different from those for which they were first collected**. Clearly, this secondary use is in conflict with the purpose limitation principle set out in the data protection Directive.

❖ **Cloud computing**

Internet services and applications are increasingly moving towards so-called “cloud computing”²³. In cloud computing models, infrastructure and software are no longer owned or controlled by the users. Instead, companies which engage in cloud computing purchase computer resources as a service. The provision of services is delegated to third parties and thus the customer (data controller) also delegates the control over the data that is being processed.

The most important difficulty posed by cloud computing services is the fact that the user and the customer (data controller) loose control over the data, which is hosted in servers located anywhere in the world. This represents a **challenge in**

²¹ Among other things, these services offer means for users to interact based on self-generated personal profiles, which support an unprecedented level of disclosure of personal information about the individuals concerned.

²² By default, information posted on Facebook can be seen by everyone. As explained in the terms and conditions: “*any information that's visible to everyone may be seen by everyone on the Internet. It will be visible to anyone viewing your profile, and Facebook-enhanced applications and websites that you use will be able to access it. Additionally, it may be visible in search engines or through RSS feeds*”.

²³ Cloud computing is a way of using the web where services and applications come from the “cloud” (the Internet). For instance Google currently provides a number of Cloud Computing Services, including email (“Gmail”), online document editing and storage (“Google Docs”), integrated desktop and internet search (“Google Desktop”), online photo storage (“Picasa”), and scheduling programs (“Google Calendar”).

terms of liabilities over eventual breaches of data protection laws²⁴. Cloud computing also raises a challenge in relation to the rules on **cross-border transfers of data**²⁵. Because the data can be stored anywhere in different servers throughout the world, the EU rules on cross-border transfer of personal data (article 25 of the Directive) are almost impossible to implement.

❖ Deep Packet Inspection

Techniques that facilitate the tracking and inspection of the content of personal electronic communications are becoming increasingly sophisticated. One of these techniques is Deep Packet Inspection (DPI).

DPI is usually described as the practice of Internet Service Providers (ISPs), or an entity working together with an ISP, monitoring the content of “packages”, not just the destination IP addresses²⁶. DPI techniques use network equipment to intercept and modify, examine, restrict, or copy the content of data communications²⁷.

We are concerned that DPI techniques can lead to a breach of a user’s privacy. There are reports that governments have utilised DPI techniques to carry out internet censorship programmes (e.g. China and Iran) and commercial entities have used this technology to monitor user behaviour so as to serve targeted ads.

We believe that DPI technologies clearly invade the privacy of user for two reasons:

1. It is the content of communications that is being intercepted not only the addresses; this breached the fundamental right to the confidentiality of correspondence and communication;
2. The public has no means to see what the broadband providers are actually doing, as DPI operates invisibly (no transparency)²⁸; network providers hide notices about DPI in incomprehensible privacy notices.

We therefore believe that **DPI techniques** are incompatible with the fundamental rights to the confidentiality of communication and to privacy and thus **should be banned**²⁹.

²⁴ See EPIC (Electronic Privacy Information Center) complaint against Google and cloud computing services before the Federal Trade Commission (FTC), March 2009: <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>

²⁵ See ENISA (European Network and Information Security Agency) report on cloud Computing, November 2009: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/>

²⁶ Each packet that is sent across the network contains a *data section* (containing the actual data being sent) and a *header section* (providing information about the source and destination of the packet, similar to how a letter envelope contains the names of the sender and of the addressee): see “European Study on the Legal Analysis of the Single Market for the Information Society”, by DLA Piper for the European Commission.

²⁷ <https://nodpi.org/> - In 2008, the UK Digital Media Company, Phorm faced severe criticisms for its practices of targeting and profiling which were believed to be based on deep packet inspection technology.

²⁸ See Office of the Privacy commissioner of Canada: <http://dpi.priv.gc.ca/>

²⁹ Please note that Which? does not agree that DPI should be banned.

PART II - SOLUTIONS

Having mapped out the problems consumers face with the current Directive, the following section will focus on what we believe to be possible solutions, largely complementary, that will help shift back the balance of powers between data controllers and data subjects – in favour of the latter.

I. The current legal framework: what is to be maintained, what needs to be changed

❖ Positive impact of the Lisbon Treaty on data protection and privacy

First, before considering the revision of the framework Directive, it is important to acknowledge the changes that will be brought 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 need to be fully complied with by both the EU institutions and Member States, acting within the scope of the EU law³⁰.

❖ The core principles of the Directive must be maintained

The European principles provide a high level of protection, setting the standards adopted by several other countries and the foundations of international instruments – including the recent ‘Madrid Declaration’³¹.

We fundamentally believe that the existing **core principles of the Directive** - fair and lawful processing, purpose limitation and specification, data minimisation, consent, right to access, object, correct and withdraw one’s data to name a few - **remain relevant and must be retained**. While the focus today is often related to data protection and privacy online, it is equally important to keep **technology neutral** principles.

Moreover, many aspects of the Directive have not been explored to their full potential – let alone the poor level of compliance and enforcement. Indeed, we find it difficult to accept the arguments that the Directive does not fit to the online environment when the Directive is currently not complied with by various online players. Just because the future of the Directive is currently being discussed, it does not follow that it should no longer be complied with.

II. How to address existing challenges?

We have identified several fields that would allow the Directive to be more effective in protecting consumers’ data and privacy. The points developed below require the

³⁰ The UK and Poland opted out of the EU Charter.

³¹ 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.

investment and commitment of all stakeholders – authorities, businesses and consumers alike.

1. Improve the enforcement of the Directive

The level of compliance with and enforcement of the Directive – both offline and online is far from being exemplary³². This may in part be due to different interpretations by Member States of the Directive, and poor or uneven implementation. We believe that enforcement can be fostered through technical solutions but also through actions by Data Protection Authorities (DPAs) and other relevant authorities, by data subjects and by business players.

❖ **By implementing technical solutions: have “privacy by default” to avoid “privacy by disaster”**

First, compliance and enforcement can be fostered through technical means and technological solutions. We firmly believe that **privacy and security by design** - i.e. building security and privacy from the very beginning in the design specifications of systems and technologies and from end to end – is necessary. As Peter Hustinx, the European Data Protection Supervisor, recently stated: *"Real security does not exist without the privacy built in, and privacy in a networked world is not possible without security measures"*³³.

Such technical solutions could help 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 privacy³⁴.

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 standards³⁵. We are convinced that technical solutions to privacy are cost-effective as they mitigate the risks from the very beginning, avoiding the fixing of problems at a later date, usually a far more costly option which often goes hand in hand with reputational damage and questioned credibility. An integrated risk management approach is imperative.

Privacy and security by default is also a way to enhance consumer control and facilitate consumer choice. In addition, such technical solutions would facilitate the notification and verification procedures by the DPAs.

³² Only 13 % of the people responsible for data protection within companies said they were very familiar with the provisions of the data protection law. Only 48% of citizens thought that their data was properly protected in their own country (Eurobarometer survey on data protection in the EU, February 2008).

³³ Peter Hustinx speech at the seminar on "Responding to data breaches", 23 October 2009.

³⁴ 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/>

³⁵ Regarding standards, please refer to ANEC answer to this consultation, ANEC-ICT-2009-G-086.

A good basis can already be found in **article 17 of the Directive** requiring “*appropriate technical and organisational measures*” to protect personal data³⁶. This provision **should be interpreted to give legal foundation to privacy by default**. However, it is important to note that the necessity for embedded protection in the design has already been acknowledged by the European Commission for specific domains like RFID or the Internet of Things³⁷. It should be recognised as a general principle of better enforcement and control.

❖ **By business players**

It goes without saying that data controllers are the first responsible for complying with the Directive. In addition to the use of technical solutions as described above, we believe that **Privacy Impact Assessments (PIAs) and audits/controls should be made compulsory** for both data controllers and data processors – the latter should be seen to take more responsibility.

Both are recognised in the Madrid Declaration³⁸ as proactive measures for better compliance. The Declaration foresees “*periodic conduct of transparent audits by qualified and preferably independent parties*” but also the implementation of PIA “*prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modification of existing processing*” – as already foreseen in the European Commission Recommendation on RFID³⁹.

It is important to note that there should never be a “once and for all” approach to privacy; information systems and technologies will need to be adapted to ‘state of the art’ throughout their lifecycle.

Software and systems must be designed with privacy and data protection compliance features (privacy by design⁴⁰). In addition, **prior testing** should also be considered. Products should be road tested before they are put on the market to ensure they meet privacy and security standards. Moreover, the regular **training of staff** on privacy and data protection issues (including services and products developers) should be encouraged. In addition, the compulsory **appointment of a data protection officer** in companies collecting and/or processing personal data as it is already the case in Germany, should be considered. Similarly, DPA could organise cheap **training for SMEs** that cannot afford to hire a data protection officer.

Self-regulation could also play a complementary role in making the Directive more effective.

³⁶ And also in Recital 46 of the Directive.

³⁷ E.g. Communication of the European Commission on *the Internet of Things* - An action plan for Europe, June 2009.

³⁸ 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. See point 22.

³⁹ European Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, May 2009.

⁴⁰ *Privacy by Design* is a concept that was developed by Ontario’s Privacy Commissioner, Dr. Ann Cavoukian, back in the 90’s, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems: <http://www.privacybydesign.ca/>

❖ **By data protection authorities/consumer authorities**

We believe that **Data Protection Authorities (DPAs) must be given the means and the tools to fulfil their mission**. They should be independent, impartial, have the technical competence, sufficient powers and adequate resources to control and sanction.

Last year the German Federation of Consumer Organisations (vzbv) was able to buy six million sets of consumer data on the black market for 850 Euros. The seller of this data was only punished with a fine of 900 Euros. The **sanctions** DPAs can impose need to have a **clear deterrent effect**⁴¹.

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.**

In any case, authorities’ action should never preclude the right of consumers to take action.

❖ **By empowering data subjects**

Consumers’ empowerment and control is at the very heart of the Directive. It cannot be inferred that consumers do not care about their privacy simply because they do not exercise their rights or do not actively create content online⁴². Today, there is an increasing trend towards asymmetry of information and data centralisation, resulting in the shift of control away from consumers.

The best way to ensure consumers’ control is to ensure that consumers can exercise their rights easily and at various levels. In the online world, consumers should have the possibility to **exercise their rights freely and by email/via electronic means** – and not by snail mail as it is most often the case today, which creates an asymmetry of rights/duties and an extra burden on the data subject.

In addition, **privacy campaigns** should also be run by consumer organisations and data protection authorities to raise awareness amongst consumers about their rights and obligations. Appropriate resources to carry this important task should be granted to both.

While there is a role for better information and education of consumers, one should be **careful not to put the full responsibility on consumers’ shoulders**. Consumers need to be given the tools to better enforce their rights – starting with easily accessible complaint procedure mechanisms and access to data processors.

⁴¹ For instance, a consultation on custodial sanctions for those found guilty of knowingly or recklessly obtaining, disclosing, selling or procuring the disclosure of personal data without the consent of the data controller is currently on-going in the UK.

⁴² See for instance the results of the Eurobarometer survey on data protection in Europe (February 2008) or of the Scientific report 'Young People and Emerging Digital Services', 2009.

Consumer organisations should be given the support and resource to build a local system of accountability agents to help individuals exercise their rights and act as a means to prioritise workload for DPAs⁴³.

The 'Madrid Declaration' foresees a "direct recourse to the courts" for data subjects⁴⁴ to enforce their rights. Business should also **compensate consumers for any detriment they may suffer as a result of data breaches or unauthorised use of data.**

Given the relatively low amount of money involved and the fact that moral damages are difficult to quantify, consumers will not go individually to court. A **collective judicial redress instrument** ("group action") in Europe will ensure that consumers can exercise their right to be compensated for the damage they have suffered. If such a measure existed, it would also provide an incentive for companies to abide by the law.

2. Ensure fairness and transparency

Transparency is key. It is indispensable to comply with the obligations of the Directive, to raise awareness, to foster trust, to empower users and to ensure accountability. But transparency does not simply mean displaying information – e.g. pages and pages of legalese as it is the case today with privacy notices. Transparency should also be interpreted beyond privacy notices; notice should be before or at the point of collection wherever it is collected.

❖ **By guaranteeing privacy notices are transparent, fair and accessible**

*"The burden placed upon individuals to read these policies stretches the limits of acceptability"*⁴⁵. How do you want consumers to evoke their rights when they do not know in the first place that their data are being collected and processed? Existing privacy policies discourage people from reading all the obligations forced upon them and exercising their rights.

For instance, today, consumers give away their personal data for use of a service online and the advertising company reaps the economic benefit. Internet users are thus paying for services with their personal data. We are not inherently opposed to consumers entering such an exchange for a free service, or other tangible benefit, but it must be ensured that it is absolutely transparent from the outset that this exchange is taking place, that the data is being collected, what it will be used for and how long it will be retained.

Fairness of terms needs to be improved and policy notices must be easily accessible and clearly displayed in plain and intelligible language. Notice must be provided at the point of collection (including secondary purposes, whether data is shared with or sold to third parties, who these third parties are and what they intend to do with the data...). In addition, the industry must find adequate

⁴³ RAND report Europe 'Review of the Data Protection Directive' (May 2009): http://danskprivacynet.files.wordpress.com/2009/05/review_of_eu_dp_directive.pdf

⁴⁴ Point 23 of the Madrid Declaration.

⁴⁵ The London School of Economics and Political Science (LSE), from legitimacy to informed consent: mapping best practices and identifying risks, a Report from the Working Group on Consumer Consent, May 2009.

technologies aiming to facilitate compliance with the principle of meaningful consent of the data subject. This point was also underlined in the Madrid Declaration⁴⁶.

Several options could be explored to improve transparency such as 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 informed consumers is.

Back in 2004⁴⁷, the Article 29 Working Party already proposed to use language and layout that is easy to understand by users, especially for people with particular needs (e.g. children) and multi-layered format notices. We believe 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.

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 burden to demonstrate that consumers are well-informed should be on the business.

3. Foster strong public accountability

As rightly stated by Commissioner Reding: *"Those who profit from the information revolution must respond to the public policy responsibilities that come with it"*⁴⁸. A **strong** sense of **public accountability** needs to be developed amongst data controllers and data processors⁴⁹. As described above, the design of products and transparency make accountability more effective; but additional measures should be taken.

❖ By introducing a general data breach notification system

Data protection, privacy and security go hand in hand. The Directive foresees an obligation on the data controller to take appropriate security measures to protect the data he stores⁵⁰.

Despite this security obligation, more and more data breaches make it to the front pages of newspapers – which only reveals the top of the iceberg. A recent study finds that 67% of French organisations were hit by one or more data breach incidents within the last twelve months. However, a massive 92 percent of the data breaches were never disclosed as there was no legal or regulatory requirement to do so⁵¹.

⁴⁶ Point 10.6 of the Madrid declaration.

⁴⁷ Article 29 Working Party Opinion 10/2004 on More Harmonised Information Provisions

⁴⁸ Commissioner Reding speech on Securing personal data and fighting data breaches, 23 October 2009.

⁴⁹ See for instance point 11 of the Madrid declaration.

⁵⁰ Article 17 on security of processing.

⁵¹ 2009 Annual Study: France Enterprise Encryption Trends study:

<http://www.reuters.com/article/pressRelease/idUS128891+09-Sep-2009+PRN20090909>

We are convinced that **horizontal rules concerning the prevention, management and reporting of data breaches** – not just in the electronic communications sector – **are needed**. We therefore welcome the Commission announcement to launch a consultation on a generally applicable breach notification requirement⁵².

❖ **By setting up a joint and several responsibility rules between a business and third parties in case of breach**

The chain of responsibility and liability is getting difficult to follow as the relations between data controllers and data processors – but also with third parties - are increasingly complex (e.g. cloud computing).

All actors should have a share of responsibility in ensuring that the data which circulates, is being collected and processed, is secured.

If a consumer wants to exercise his/her rights, he/she will turn to the business he/she has been in contact with; in the online world, it would typically be the website portal.

Thus, if a consumer asks the business he/she was in contact with to rectify or delete his/her data, the business should also notify this fact to third parties to whom personal data had been disclosed⁵³. 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 lie with the service provider.

Therefore, we believe that the Commission should 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 them⁵⁴.

4. Clarification and harmonisation of existing rules

In an increasingly more and more borderless and international context, several key legal questions arise: which law is applicable? Which jurisdiction is competent? In particular, at European level, the questions of national implementations of the Directive and interpretation of the key concepts are recurrent.

❖ **Applicable law**

As pointed out above, many companies based outside the EU still claim they are not subject to European law but to their national law.

⁵² Commissioner Reding speech on securing personal data and fighting data breaches, 23 October 2009:

http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20091023.pdf

⁵³ Also foreseen in point 17 of the Madrid Declaration.

⁵⁴ 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.).

When dealing with the issue of the applicable law, it is essential to keep in mind that the primary aim of the Directive is to protect the interests of the citizens whose data is being collected and processed⁵⁵. Besides, an Internet user does not necessarily always know whether the website he will visit and provide data to (either unknowingly or consciously) is situated in the EU or elsewhere.

The issue has been analysed by the **article 29 Working Party**⁵⁶, which states that the “use of equipment” criterion must be interpreted extensively as including the use of the data subject’s PC, in particular when placing cookies and spyware, terminals and servers⁵⁷. **BEUC welcomes this interpretation.**

In practice, when there is an element or factor closely connected to the EU, which helps protect the interests of EU citizens, the legislator⁵⁸ and the judge⁵⁹ often decide in favour of EU law.

BEUC believes that **EU law should apply to cases where services are targeted at EU citizens**. 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 Working Party.

In this context, we have seen recently that Facebook accepted to change its terms and conditions to meet Canadian law but also, more recently, to abide by German law⁶⁰.

❖ Jurisdiction

In case of litigation, the matter should be taken **before the court in the country of residence of the data subject** - as in consumer protection law/Brussels I regulation⁶¹. A French draft law on privacy online⁶² currently under discussion also reaches the same conclusion.

⁵⁵ This is confirmed by recital 20 of the Directive with 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*”.

⁵⁶ Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30 May 2002:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

⁵⁷ Opinion 1/2008 on data protection issues related to search engines, April 2008:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

⁵⁸ 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).

⁵⁹ See ECJ jurisprudence on the Rome Convention; e.g. Ingmar GB Ltd. and Eaton Leonard Technologies Case C-381/98.

⁶⁰ See for Germany: <http://www.vzbv.de/go/presse/1234/36/102/index.html>

⁶¹ See Article 16.2 of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

⁶² Proposition de loi visant à mieux garantir le droit à la vie privée à l’heure numérique, November 2009.

❖ International standards

We welcome the International standards on the protection of personal data and privacy – so called ‘Madrid Declaration’⁶³ that were recently adopted and supported by both civil society and private corporations. We believe it is a first step towards the development of a set of binding international privacy principles. Nevertheless, we believe that national and regional legislation still remains relevant and necessary.

❖ The role of the Article 29 Working Party

When it comes to harmonisation, especially of key terms such as ‘consent’ or ‘legitimate interests’, we believe that the Article 29 Working Party has a major role to play and that its opinions should be given more strength. They should be fully reflected in Commission proposals and should be put into guidelines by national DPAs for a better coherence 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 should clarify privacy standards and the role of ‘privacy by design’ for new technologies and business models that will foster compliance⁶⁴.

5. Introduce new rights specific to the Digital Age

We take the opportunity of this consultation, to raise the need to develop new rights in view of the new challenges raised by the information society. We believe that the general data protection framework Directive should remain technologically neutral and that such rights should be introduced **in a new instrument**.

❖ The right to “be forgotten”

Everything posted online may stay there for perpetuity, in some form or another – through Internet archives websites or search engines caches⁶⁵ - even posts or pictures one thought no longer existed. This is even more relevant for young people; would they want appalling photos taken at parties 10 years earlier popping up on the Web to be seen by their future employer?

We believe that a **general right to “be forgotten” on the Internet should be introduced** similar to a right to “the silence of the chips”/“to be left alone” which has been called for in the field of RFID/Internet of Things.

A French draft law⁶⁶ proposes such a right - “droit à l’oubli” - that could help develop the idea further. In the draft, this right would be implemented through:

⁶³ 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.

⁶⁴ RAND Europe ‘Review of the Data Protection Directive’ (May 2009):

http://danskprivacynet.files.wordpress.com/2009/05/review_of_eu_dp_directive.pdf

⁶⁵ “Privacy by design...take the challenge”, by Ann Cavoukian, Ontario Information and Privacy Commissioner, 2009.

⁶⁶ Proposition de loi visant à mieux garantir le droit à la vie privée à l’heure numérique, November 2009.

- an obligation to inform the data subject in a specific, clear and understandable manner on how long the data will be kept; the possibility to delete, access and rectify his/her data for free and by email/via electronic means; and on the origin of the data i.e. where the data comes from to be able to trace back the data controller that originally collected and processed the information;
- an obligation to inform data subjects about the use of cookies or if the data controller processes data that was not collected directly from the data subject.

We ask the Commission to **research how such right could be made effective in practice**, keeping in mind that it is crucial to ensure that the fundamental right to freedom of expression is carefully safeguarded.

❖ **The right to data portability**

Consumers are increasingly "locked-in" to certain online sites and 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 posted online**. Existing terms and services appear mostly to be unfair and should be changed accordingly. In addition, for this right to be effective, **interoperability between services** is required.

END