BEUC The European Consumer Organisation

The Consumer Voice in Europe

Data Protection

Proposal for a Regulation

BEUC Position Paper

Contact: **Kostas Rossoglou and Nuria Rodríguez – digital@beuc.eu**

Ref.: X/2012/039 - 27/07/2012

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

Summary

The European Consumer Organisation (BEUC) welcomes the European Commission's proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). We agree with the general direction taken by the European Commission, acknowledging that while the objectives of Directive 95/46 remain relevant, a thorough review has become indispensable owing to the technological and social changes which have occurred in the digital environment.

Overall, the draft Regulation addresses the main challenges and the shortcomings of the current framework with the aim of enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of constantly evolving ICT developments.

Although the proposal in general constitutes a major improvement for individuals, a number of provisions still need to be clarified or modified to ensure the new EU framework is effective and becomes the global standard of personal data protection and privacy.

Our key concerns and our suggestions to further improve the Commission's proposal are summarised below:

General provisions	**Material scope** (art. 2) We welcome the general scope of application. Yet, the exceptions to the scope should be clearly defined to ensure legal certainty and uniform application of the Regulation: - the exception on activities related to "national security" should be further defined; - The exception on household activities should not apply when data is made available to an indefinite number of people. **Territorial scope** (art. 3) We welcome that the Regulation applies to controllers established in and outside of the European Union (when processing personal data in the EU). - For controllers established in the EU, the Regulation should address the issue of national applicable law. - For controllers not established in the EU, the application of the regulation to the "monitoring of behaviour" of data subjects must be clarified, to ensure that it includes tracking and profiling of data subjects as well as services which are based on monetizing the secondary use of consumers' personal data. **Definitions** (art. 4) "Personal data":

	BEUC welcomes the broad definition of personal data as reflected in the proposal as it will provide the necessary flexibility in the light of rapid ICT developments. In order to ensure legal certainty, it should be clarified that when there is a close relation between the data and an individual that singles out the individual, this will trigger the application of data protection rules. "Consent": BEUC welcomes recital 25 stating that consent can be given by any appropriate method and that electronic consent should not hinder the data subject's on line experience. There is no 'one size fits all' solution to the issue of consent but consent must always be meaningful. In addition, compliance with the principles for data processing including data minimization and purpose limitation needs to be ensured. "Main establishment": We welcome the definition of "main establishment" of the controller. However, the regulation should address the case of undertakings with decentralized decision making structure: in these cases the main establishment of the group may be used as the determining factor, or alternatively the dominant influence of one establishment over the others. "Transfer" of personal data (new) A definition of what is to be considered as "transfer" of personal data needs to be introduced in relation to the exchange of data between companies in the same country and other types of exchanges on networks, such as servers of companies.
Principles	(Arts. 5, 6 and 7) BEUC welcomes the introduction of the principle of transparency and the strengthening of the data minimization principle; As regards the principle of purpose limitation, a clear definition of what is to be considered as "compatible" use with the initial purpose of processing needs to be introduced; The concept of legitimate interests of the data controller must be clearly defined; it should not be left to a delegated act, as there is a risk of surpassing the legal grounds;
Special categories of data	**Personal data of a child and sensitive data** (arts. 8 and 9) BEUC welcomes the requirement of parental consent for the processing of personal data of a child. However, verification procedures of parental consent should not lead to further processing of data which otherwise would not be necessary

	to process. BEUC welcomes the prohibition of collection/processing of sensitive data as the general rule (article 9). The list of sensitive personal data must remain exhaustive and also include financial data revealing personal solvency.
Rights of the data subject	**Transparency** (art. 11) BEUC welcomes the new requirement that information has to be provided in an intelligible form and using clear and plain language. **Modalities for exercising of rights** (art. 12) BEUC welcomes the requirements in article 12 of the proposal: - Data controllers are required to respond to requests by data subjects without undue delay and no later than one month; - Data controllers will not be able to charge for the data subject's exercise of his rights, as long as this right is not abused. **Rights in relation to recipients** (art. 13) BEUC welcomes the introduction of an obligation for the data controller to notify each recipient (third parties) to whom data has been disclosed, in case of request of rectification or erasure by the data subject. **Information to the data subject** (art. 14) The list of information obligations of the controller is rather comprehensive. BEUC suggests adding the following items to the list: - the type of personal data collected and processed: - the procedures to lodge complaints; - whether processing is done for tracking and profiling purposes and its consequences on individuals; - which personal data is obligatory to provide and which is voluntary; - Where applicable, the information that personal data is collected in exchange for so-called "free services". **Right to be forgotten** (art. 17) BEUC supports the intention of the "Right to be forgotten" which aims to strengthen the right to erase personal data. It should be made clear that the obligation to delete the consumer's data lies upon the controller of the information and not upon the downstream parties (host providers, search engines etc), in order to ensure the compatibility with the provisions on the liability of Internet Service Providers under the Directive on e-commerce. **Right to data portability** (art. 18) BEUC welcomes the introduction of the new right to data portability. The right to data portability allows the consumer

	to be in control of his data and retain the ownership, by being able to shift the data to other services. Yet, for this right to be effectively implemented the development of interoperable or compatible standards is necessary. **Right to object** (art. 19) It should be clarified that the right to object, if upheld by the controller should result in the deletion of the data by the controller. **Profiling** (art. 20) BEUC welcomes the specific inclusion of profiling practices in the proposed regulation. In addition to the right not to be subject to profiling, consumers should be informed of the techniques and procedures used for profiling and the possible consequences of profiling techniques applied to them. Profiling of vulnerable consumers such as children should be prohibited. **Restrictions** (art. 21) BEUC considers that the conditions and guarantees under which the rights of the data subject may be restricted must be explicitly and further defined.
Controller and processor	**Responsibility of the controller** (art. 22) BEUC welcomes the provisions on controller's responsibility and accountability. However, the principle of accountability should not be perceived as an alternative to compliance with legal obligations or as an excuse to avoid administrative sanctions. **Data protection by design and by default** (art. 23) BEUC very much welcomes the introduction of the principles of data protection by design and by default; the following requirements should be added: - Reference to the use of Privacy Enhancing Technologies (PETs) should be introduced, as a tool to implement technical solutions to comply with the principle of data protection by design. - The principle of Data Protection by default should be revised to make it explicit that the privacy settings on services and products should by default comply with the general principles of data protection, such as data minimization and purpose limitation; - The data processor should also be obliged to implement privacy by design and privacy by default when processing personal data on behalf of the controller. **Joint controllers** (art. 24) BEUC welcomes the obligation of joint controllers to define their respective responsibilities for compliance with their obligations, by means of an arrangement between them. We would also suggest introducing the principle of joint responsibility between the controller and the processor.

	Representatives of controllers not established in the Union (art. 25) BEUC welcomes the requirement for controllers not established in the EU to designate a representative in the Union. The representative is expected to be the contact point for both data protection authorities and the data subject. Any exceptions to this requirement must be fully justified or otherwise deleted. **Documentation** (art. 28) The obligation to maintain documentation as defined in this provision is welcome and should not be weakened: it includes the most relevant information which should ensure that controllers are able to demonstrate compliance upon request by the DPAs. **Data breach notification** (art. 31) BEUC welcomes the introduction of a horizontal data breach notification obligation. - Only those breaches that adversely affect the individual should be notified to data subjects. - BEUC supports a risk-based definition of the adverse effect of data breaches. - The notification to data protection authorities must take place as soon as possible without undue delay, and not beyond 72 hours after the controller becomes aware of the data breach. - A specific deadline must be introduced for the DPA to act on a breach notification, as well as a deadline within which the data controller should notify the breach to the data subject. **Data Protection Impact Assessment (DPIA)** (art. 32) BEUC welcomes the introduction of the obligation to carry out an assessment of the impact on the protection of personal data of the processing operations that present specific risks. - A DPIA should also be carried out when processing operations "are likely" to present specific risks to the rights and freedoms of data subjects; - The DPIA should be made publicly available, or at least a summary of it; DPIAs must be audited by Data Protection Authorities. **Data Protection Officer** (arts 35-37) BEUC welcomes the introduction of the obligation to appoint a Data Protection Officer (DPO). Only those entities that are processing personal data as an accessory activity could be excepted from this obligation. The independence of DPOs needs to be strengthened.

	Exception for SMEs BEUC is opposed to the exceptions from specific obligations for enterprises with less than 250 employees. The determining factor for introducing an exception should not be the number of employees but the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data about. **Codes of conduct** (art. 38) Self regulatory codes can only be endorsed if they entail an added value for consumers' rights (by offering a higher level of protection), are backed up by suitably robust auditing or testing procedures and provide for independent and effective complaint handling and sanctions. **Certification** (art. 39) BEUC supports 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. It is also important to clarify that the granting of a seal would not simply certify compliance with the law but also offer an added layer of protection.
Transfer to third countries	(Arts 40-45) BEUC welcomes the provisions on transfer of data to third countries. However, transfers should not be possible for those countries for which the European Commission has already adopted a decision not recognizing the adequate status. Derogations from "adequate decisions" or "appropriate safeguards" must only apply for a restricted number of cases of occasional transfer that cannot be qualified as frequent, massive or structural. Disclosure of personal data to law enforcement authorities of third countries must only be possible upon prior authorization by the supervisory authority.
Supervisory Authorities	(Arts 46-54) BEUC welcomes the provisions that require explicitly the independent status of supervisory authorities The establishment of a "one stop shop" for data controllers or processors might result in forum shopping; effective coordination between all relevant DPA should be ensured. Specific rules on the assignment of a lead authority when the controller is not established in the EU should also be defined. Specific rules of allocation of financial resources to DPAs must be introduced.

Cooperation and consistency	(Arts 55-63) BEUC welcomes the focus of the draft Regulation on enhancing cooperation between data protection authorities; strengthening cooperation and coordination is crucial as a data breach may well affect data subjects in many countries across the EU and beyond. However, the possibilities to trigger the consistency mechanism go too far. There needs to be a threshold in the draft Regulation to ensure that the consistency mechanism only applies to processing that raises serious risks to data subjects across Europe. The powers of the European Commission within the consistency mechanism must be carefully drafted in order not to undermine the independence of DPAs.
Remedies, liabilities and sanctions	(Arts 73-79) Judicial collective actions for compensation by representative bodies should be introduced. Consumer organizations must be entitled to bring actions for breaches of data protection law. Part of the fines imposed on companies should also be used to finance the actions of organizations defending the rights of data subjects.
Specific situations	**Processing of personal data and freedom of expression** (art. 80) BEUC welcomes the exemption from the application of the regulation when personal data is processed for journalistic purposes or for the purpose of artistic and literacy expression. The notion of journalistic purposes should be clarified to include not only the traditional media, but also new activities whose object is the disclosure to the public of information, opinions or ideas. **Processing of personal data concerning health** (art. 81) The use of sensitive health data for marketing purposes should remain prohibited. Tracking and profiling technologies in health related web sites should not be allowed. Only authorised and specifically trained health care professionals should be allowed to have access to patients' health records.
Delegated and implementing acts	BEUC regrets that too many issues in the draft Regulation are left to be dealt with by delegated and implementing acts. The number of delegated and implementing acts should be cut down and limited to those provisions addressing non-essential issues, such as design requirements or criteria for technical measures.

Introduction

The European Consumer Organisation (BEUC) welcomes the European Commission's proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). We agree with the general direction taken by the European Commission, acknowledging that while the objectives of Directive 95/46 remain relevant, a thorough review has become indispensable owing to the technological and social changes which have occurred in the digital environment.

Overall, the draft Regulation addresses the main challenges and the shortcomings of the current framework with the aim of enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of constantly evolving ICT developments. The European Union needs a consolidated, general framework which applies across the board and which can then be complemented by more specific rules as necessary.

The revision of the current framework also acknowledges 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 protection of personal data and privacy, will now need to be fully complied with by the EU institutions and Member States, acting within the scope of the EU law.

Although the proposal in general constitutes a major improvement for individuals, a number of provisions still need to be clarified or modified to ensure the new EU framework is effective and becomes the global standard of personal data protection and privacy.

The on-going revision should not result in the reduction of protection. BEUC wishes to highlight that the adoption of a user-centred approach and the placement of data subjects at the forefront of considerations constitutes a *sine qua non* requirement to achieve the objectives of the EU Digital Agenda, which aims to build consumer trust in the online environment. The revision should not be used as an opportunity to weaken fundamental principles of data protection.

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

It must also be borne in mind that the European framework for data protection has been used as a global standard and has provided a basis for the development of legislation in other countries. The EU should therefore respond to the expectations of citizens and consumers in Europe and beyond.

CHAPTER I – GENERAL PROVISIONS

Article 2 – Material scope

Article 2 of the proposal defines the material scope of the regulation in the same terms as Directive 95/46: it applies to "*the processing of personal data wholly or partly by automated means or to the processing of non-automatic means of personal data which forms part or is tended to form part of a filling system*."

However, the exceptions to the general scope are broader in the proposal than in the current Directive. While we do not oppose the exceptions, we assert that they must be better defined to avoid different interpretations and undue use of personal data in borderline cases.

With regard to the exception of **national security**, we would like to highlight that the scope of this notion often differs from one Member State to another, which will undermine the uniform application. Thus, we think that the Regulation should introduce certain criteria which better define the extent of this exception.

With regard to the exception of **personal and household activities**, we welcome the reference to the gainful interest as the main criterion for the application of the exception. The question of whether individuals processing data for personal and household activities is particularly important within a technological context, with individuals posting content online via social networking sites, blogging sites etc. We would however recommend including in Article 2 the elements of the definition of "gainful interest" provided in Recital 15, namely that the notion is linked to professional or commercial activity.

Furthermore, the draft Regulation does not clarify the application of the exception when data is made available to an indefinite number of individuals. According to the case law of the European Court of Justice[1], the exception should only apply when the data is made available to a limited number of individuals. We would therefore suggest that the exception of Article 2.2.d be complemented with the criterion of indefinite number of people, thus clarifying that an indefinite number of individuals shall in principle mean that the household exception no longer applies

Article 3 – Territorial scope

Article 3 deals with the territorial scope of the proposal, addressing when the data controller is established within or outside the European Union.

Article 3.1 introduces the criterion of **establishment in the EU** to determine whether EU law would apply. However, the definition of the establishment, as the place where the main decisions as to the purposes, conditions and means of processing are taken (Article 4.13) is not appropriate for undertakings with a decentralised decision making structure, such as where the locations of where central administration and management decisions on data processing differ.

[1] See ECJ 6 November 2003, Lindquist and Satamedia, C-101/0.

Furthermore, Article 3.1 only provides for the application of EU law without any criteria to determine which national law shall apply. In principle this is logical as the Regulation is supposed to be a self-standing instrument. However, the Regulation leaves some scope for the application of national law in some of its provisions and Member States maintain the freedom to adopt specific legislation in a limited number of areas. The draft Regulation only provides for criteria to define the leading Data Protection Authority (Article 51) where several Member States are concerned, but does not address the issue of applicable national law.

Article 3.2 refers to instances where the data controller is **not established in the EU**, but the processing activities are related to the offering of goods and services to data subjects residing in the EU or monitoring their behaviour. Compared to Article 3 of the current directive, this new provision takes away the criterion of "use of equipment".

BEUC welcomes the new criteria that will ensure that consumers will be protected against the collection and processing of their personal data by companies not established in the EU; the current criterion of "equipment" has often turned out to be an obstacle to the enforcement of European law against such companies. In order to ensure more legal certainty, we believe that further clarification is needed to ensure that the offering of goods and services also includes so-called 'free services', which are based on monetising the secondary use of consumers' data[2].

We would also suggest that the meaning of "monitoring of behaviour" is clarified to include tracking and profiling done by controllers outside the EU. For these provisions to deliver benefits to European consumers, effective enforcement mechanisms and procedures need to be in place.

Article 4 – Definitions

- Article 4.1- Definition of "data subject" (personal data)

Compared to the present Directive, the criteria in the new proposal for the definition of "personal data" are transferred to the definition of "data subject". The main elements of the definitions remain in place, which BEUC welcomes. We believe the broad definition in the proposal provides the necessary flexibility to be applied to different situations and developments affecting the fundamental right of privacy and data protection in the light of rapid ICT developments[3]. It is equally important that the definition provides legal certainty as to when data is personal and the processing of which would be within the scope of the Regulation.

In particular, BEUC welcomes the fact that the new proposal widens the definition by including the concepts of online identifiers and location data. However, the proposed new definition contrasts with the wording of recital 24, according to which *"…identification numbers, location data, on line identifiers…need not necessarily be considered as personal data in all circumstances"*. This sentence undermines the

[2] Opinion 01/2012 on the data protection reform proposals by Article 29 Data Protection Working Party.
[3] The proposal follows the recommendations of the opinion of the 29 Data Protection Working Party: Opinion 7/2007 of 20 June 2007.

aim of the new definition, which is to cover any information or means allowing the identification of a data subject. As soon as the information allows the data controller to identify an individual, the information should be deemed personal data.

BEUC thus proposes the last sentence of **recital 24** to be redrafted clarifying that **when there is a close relation between the information and an individual that singles out the individual**; this will trigger the application of data protection rules.

BEUC would caution against overstretching the application of data protection rules to every single situation where information is processed, but rather its application should depend on the **specific context** and on whether the information processed can be linked to a specific person.

❖ Article 4.8- Data subject's consent

The draft Regulation establishes the consent of data subjects as one of the possible grounds for legitimising data processing. Article 4.8 requires consent to be freely given, specific, informed and explicit, while Article 7 establishes a number of conditions for consent, including placing the burden of proof on the controller that the consent requirements have been met.

BEUC welcomes the provision in recital 25 that consent can be given by "any appropriate method", which allows for a certain degree of flexibility, provided it is transparent and meaningful. We also endorse the requirement that the request to give consent in the online environment should not disrupt use of the service and should not hinder the data subject's online experience.

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 following two criteria:

- An analysis of the potential consumer detriment linked to a specific practice/ technique.
- An evaluation of whether a practice/technique meets the 'reasonable expectations' of use of information by a typical consumer or by the average member of a group when directed to several consumers.

Such an assessment will have to be done on a case by case basis. The definition of consumer expectations raises a number of challenges both in terms of the process to be followed but also in terms of constantly emerging new services, especially in the digital environment. We believe consumer associations have significant experience of deploying surveys, analysing consumer behaviour, using appropriate tools to determine consumer expectations of products and services and so can be instrumental in any regulatory work in this field.

BEUC would suggest focusing on the requirement for **consent** to be **meaningful**, while it needs to be clearly stated that consent is only one of the legal grounds for processing and not necessarily the most appropriate one in all circumstances. For example, consent cannot be valid when the requirements of transparency and information have not been met, or when collection of personal data is unnecessary for consumers to access a specific service. Consent must not lead to further

processing of data which is otherwise unnecessary. Most importantly, compliance with the principles of data protection processing, including data minimisation and purpose limitation, needs to be ensured.

- Article 4.13- Main establishment

The main establishment is defined as the place where the main decisions as to the purposes, conditions and means of processing are taken. However, this definition is inappropriate for undertakings by a decentralised decision making structure, where the locations of central administration and management decisions about data processing may differ. For those cases, the main establishment of the group may be used as the determining factor, or alternatively the dominant influence of one establishment over the others.

- Article 4.20 (new)- Transfer of personal data

BEUC regrets that the draft proposal does not provide a definition of what is to be considered the transfer of personal data. The main questions arise in relation to the passing of data between companies in the same country and other types of exchanges on networks, such as servers of companies. In a number of Member States, such transfers are prohibited and therefore the omission of this rule from the draft Regulation would result in a significant decrease of consumer protection.

CHAPTER II – Principles

Chapter II of the proposal deals with the principles of data processing and adds specific requirements for the collection and processing of data related to minors and of sensitive data. BEUC welcomes that the general principles of data processing are maintained in the proposal while significant improvements are put forward, in particular as regards the principle of transparency.

Article 5 – Principles relating to personal data processing

BEUC welcomes the introduction of the **principle of transparency** in relation to the collection and processing of data. This reflects the stronger obligations put on the controller to inform data subjects (article 14 of the proposal) about the most relevant information regarding the processing, including the identify and the contact details of the controller, the purposes of the processing, the retention period, the existence of rights and the modalities to exercise them etc., as defined in Article 14.

Lacks of transparency and information are major deterrents to users asserting 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 proposal enhances the principle of **data minimisation** by giving it more visibility in a new paragraph(e). The strengthening of this principle is necessary in order to address the current trends of data harvesting and data mining used for profiling consumers and which involve large amounts of personal data being collected.

Many data controllers who are not in a contractual relationship with consumers retain data beyond the necessary time to perform the service. In the specific case of search engines, the Article 29 Working Party required 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".

The principle of data minimisation also mirrors the new principles of privacy by design and privacy by default. According to these, data protection principles need to be embedded in privacy-sensitive technologies and services from the beginning of their development.

The principle of **purpose limitation** of data processing is of utmost importance in relation to the proliferation of business models which are construed on the basis of data sharing with third parties. The business models of many internet companies (e.g. some search engines, social networking sites…) are often incompatible with the principle of purpose limitation and the specification of use of personal data. Many companies collecting personal data transmit the data to third parties who process this data for purposes different to those initially pursued by the data controller and often without informing the data subject.

BEUC **regrets** that the concept of "compatibility" (with the original purpose of processing) is undefined in the proposal. The criterion of "compatibility" has brought about divergences at national level due to its vagueness (without specification of what is compatible or incompatible). In a few countries the principle is defined in excessively broad terms undermining the very principle. In this regard, we think that the new regulation should include some criteria as to what is considered "compatible", drawing on best practices of the way "compatibility" has been interpreted at national level.

Article 6 – Lawfulness of processing

Article 6 of the proposal reproduces the grounds for processing present in the current Directive. The processing of personal data is lawful when at least one of the following applies:

a) The data subject has given its consent to the processing,
b) Processing is necessary for the performance of a contract,
c) Processing is necessary for compliance with a legal obligation,
d) Processing is necessary to protect the vital interests of the data subject,
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of a public authority vested on the controller,
f) Processing is necessary for the purposes of the legitimate interest of the data controller unless such interest contrasts with the fundamental rights and freedoms of the data subject.

Compared to the existing directive, the proposal contains a few, but very important, novelties. The most welcome changes relate to the definition and the conditions for "consent" (Article 7) as well as the provision on the processing of personal data of a child (Article 8).

When processing is based either on controller's compliance with a legal obligation or on the public interest, the basis for the processing will have to be provided either in EU law or the national law of a Member State (Article 6.3). This provision is very important as it excludes the law of a non–EU country as the legal basis, as would be the case where processing of personal data of EU residents may be required for law enforcement purposes by third countries.

BEUC is concerned that unless properly defined, the general notion of **"legitimate interests** of the controller" might open the door to abusive processing. The concept of legitimate purposes is vague and subjective. This concept should be defined clearly in the proposal and should not be left to a delegated act, as there is a risk of surpassing the legal grounds.

Article 7 – Conditions for consent

The draft Regulation establishes data subject's consent as one of the possible grounds for legitimising data processing. Article 7 establishes a number of conditions for consent, including the burden of proof on the controller to demonstrate that the consent requirements have been met.

BEUC welcomes the provision in recital 25 that consent can be given by any appropriate method, which allows for a certain degree of flexibility, as well as the provision that the request to give consent in the online environment should not be disruptive to the use of the service and should not hinder the data subject's online experience of the service. As stated above, there is no 'one size fits all' solution to the issue of consent, while the means of implementation of consent should be flexible, user-friendly and ensure it is meaningful when it is given.

We are satisfied that Article 7 puts the burden of proof of the consent on the controller. Thus the controller should pay special attention to the reliability of the means used to obtain consent of the data subject in accordance with recital 25. We also welcome the inclusion of the right to withdraw consent at any time.

However, for consent to be valid, the conditions of informed, specific and free will have to be met. The draft regulation provides examples of cases where consent cannot be valid due to a lack of balance between the parties, for instance in the employment sector. We highlight however that the lack of balance is present also in other sectors such as the insurance sector – where often the benefit of special conditions is tied to the consent of the consumer to the processing of his/her data; recital 34 should thus add the insurance sector as an example of possible lack of balance. As regards the "informed" consent, the data subject should receive clear and understandable information (in a concise manner) on key elements which are defined in Article 14.

We are also concerned that under the proposal, the consumer may be requested to provide consent once that would cover multiple data processing operations. It is questionable whether the consumer is able to deduce the consequences and understand the implications.

Article 8 - Processing of the personal data of a child

BEUC welcomes the new provision in Article 8 requiring parental consent for the processing of personal data of a child.

In particular in the online environment minors do not always have the knowledge to realise the consequences of the collection or processing of their personal data. The internet and new technologies offer ever wider possibilities for children to share data (photos, videos, messages, localisation information through blogs, videos, social networks…) which, combined with the lack of awareness of the risks and dangers of data collecting, make children and teenagers the most vulnerable group in the digital world.

However, we see a number of problems regarding the implementation of the obligation of parental consent. First, the threshold of 13 years old might conflict with national laws relating to the legal capacity to conclude a contract, the processing of data occurring very often in the context of a contractual relationship. Second, the obligation to develop means to verify the legitimacy of parental consent, should not lead to further processing of data which otherwise would not be necessary to process. We also think that the criteria and modalities for the parental consent should not be totally left to delegated acts of the Commission; some criteria should be included in the regulation itself.

In addition this provision seems to apply only in the context of the "offering of information society services". The meaning of offering information society services seems to be too restrictive and it should be clarified; the provision should apply to any processing of personal data of a child both on and off-line.

Article 9 - Processing of special categories of personal data

We welcome the prohibition of the collection or processing of sensitive data as referred to in Article 9.1 of the proposal. BEUC believes that the list of sensitive personal data must be exhaustive to ensure legal certainty and avoid divergent implementation at national level. However, we put forward that financial data which reveals personal solvency should also be added to the list of Article 9.2 Other forms of financial data such as 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.

Finally, we believe that the specificities, conditions and safeguards for the processing of sensitive data should not be left to delegated acts of the Commission; sensitive data requires an additional layer of protection and thus the conditions for their processing need to be clarified in the regulation. Alternatively, this could be the object of opinions or reports of the European Data Protection Board.

CHAPTER III – Rights of the data subject

Article 11 – Transparent information and communication

Lack of transparency and lack of clear information is a major deterrent to users in the assertion of their rights. Consumers rarely understand privacy notices which are generally too lengthy. The privacy policies of many 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, 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 websites, while they may not be updated once they are published, even when the content and the nature of the service have evolved.

According to different surveys, although consumers are concerned about their privacy, they do not view privacy policies 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.

According to the figures provided by the Eurobarometer[4] 64% of users feel that information on the processing of their data is unsatisfactory. According to a study by the Norwegian Consumer Council[5], 73% of users aged 15-30 years seldom read Terms of privacy notices 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

The proposal significantly strengthens the information obligations of the controller to the data subject (Articles 11, 12 and 13). We in particular welcome the new requirement that information has to be provided in an intelligible form while using clear and plain language. We also support the regulation of procedures for providing the information to the data subjects as this will strengthen accountability of the controller *vis-à-vis* the data subject.

[4] Eurobarometer survey on data protection in the EU - citizens' perceptions, February 2008.
[5] http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf .

Article 12 – Procedures and mechanisms for exercising the rights of the data subject

BEUC welcomes the introduction of specific modalities for the exercise of the rights of the data subject. Data controllers should respond to requests by data subjects without undue delay and no later than one month. Furthermore, data controllers should not be able to charge a data subject for access to his own personal data, as long as this right is not abused. 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.

Article 13 – Rights in relation to recipients

BEUC welcomes the introduction of an obligation for the data controller to notify each recipient to whom data has been disclosed in case of rectification or erasure, as long as it is possible without a disproportionate effort. This provision is particularly important in the online environment, where data can be easily shared with third parties and therefore inaccuracies need to be corrected. However, we are concerned as regards the exception in cases where such communication would involve a disproportionate effort (Article 13.5.c). Such a broad and subjective condition cannot be justified, as it will always be the case that providing information might require an effort by the data controller.

Article 14 - Information to the data subject

Article 14 sets up a list of all the information the data controller is obliged to give to the data subject when his personal data has been collected. Overall this provision is comprehensive and encompasses the relevant information the data subject needs to have. However, information about the type of personal data collected and processed is currently missing from the list and should be added.

We particularly welcome the new obligation of the data controller to inform the data subject of his right to lodge a complaint to the supervisory authority and the contact details, reflecting the new right of the data subject to directly lodge complaints (Article 15.1 [f]). However, data subjects also need to know about the procedures to lodge such complaints; this should be added to the text - often consumers are not aware of the procedural steps to lodge complaints.

In addition, this provision should echo the inclusion of a specific article dealing with profiling (Article 20) by requiring information about tracking and profiling purposes and its consequences on individuals to be added under Article 14.1 b.

Regarding the exceptions to the information obligations listed in Article 14.5, we think that the exception in Article 14.5b (when the information to the data subject proves impossible or carries a disproportionate effort) should be better defined in the regulation, instead of letting the Commission adopt delegated acts to specify such exception. The provision of information will always require an effort from the data controller, which he may claim is disproportionate.

It is equally important to inform the data subject which personal data is obligatory to provide and which is voluntary. As regards services whose business model is based on monetising the use of consumers' personal data in exchange for so-called 'free services', it should be made crystal clear to the consumer that this exchange is taking place, while the processing of data should comply with the general principles of data minimisation, purpose limitation etc.

We support the reference to standard forms to lay out the information provided to the data subject, but we think this should be a requisite rather than optional. Standard forms generally offer better and more structured information to consumers. We also think that the new European Data Protection Board (EDPB) should take the lead in developing such standard privacy notices alongside consumer representatives and businesses.

Finally, the possibility for data controllers to present the information by using multi-layered notices should be expressly allowed.

Article 15 - Right of access for the data subject

Article 15 includes a list of information obligations in relation to the right of the data subject to access at any time the processed data. Compared to the current Directive, the addition of the obligation to inform about the right to lodge a complaint with the supervisory authority and its contact details (15.1 (f)) is very welcome. Yet, as said above, data subjects should also be informed about the procedures to lodge complaints. Consumers cannot fully benefit from their rights if they are not informed about the ways to complain and to obtain redress where there have been infringements.

Article 17 - Right to be forgotten and to erasure

The digital print left by individuals when personal data is processed online is problematic for consumers; consumers may well wish to erase the traces they leave behind on the Web at one point in time. The consumer should be able to delete the information provided to a company when the data is no longer necessary or when he withdraws consent.

BEUC supports the intention of the 'right to be forgotten' which aims to strengthen the right to erase personal data. Even though the right of erasure is included in the current directive, its application in the online environment is very often ignored.

The new Article 17 should allow better enforcement of the existing right of erasure in the digital environment. Indeed, according to the new proposal the controller will be held liable in case he has made the personal data public or has authorised the processing of the data by third parties.

Users have the right to expect online companies to delete their personal information upon request. For example, users of social network services, email services, and other similar services should not worry that companies will retain their information after they are no longer users of the service. With respect to search companies, users might also reasonably expect that personal information, acquired by the company for commercial gain, should not be republished where the user has made an explicit request.

However, we consider the naming ("forgotten") to be misleading as the limitations of a "right to be forgotten" are manifold and have to be acknowledged. It should be made clear that the obligation to delete the consumer's data lies upon the controller of the information and not the downstream parties (host providers, search engines etc.), in order to ensure compatibility with the provisions on the liability of Internet Service Providers under the Directive on e-Commerce. The implementation and enforcement of the right to be forgotten must not result in the application of technical measures resulting in the filtering of online communications. The relationship with the provisions of the e-Commerce Directive on the liability of information service providers needs to be carefully assessed.

Moreover, in many cases it would be impossible to inform all parties to whom data has been disclosed and track down all possible links and copies of data. In this regard, Article 17.2 should be understood in the sense that only an obligation of effort is imposed on the controller and not an obligation of result. To this end, different metadata techniques which could convey the information regarding the appropriate use of the data could be used.

Finally, the requirements, conditions and criteria for the implementation of the right to be forgotten should not be left to delegated acts of the Commission but should be defined in the regulation.

Article 18 - Right to data portability

BEUC very much welcomes the introduction of the new right to data portability in the proposal (Article 18). In the online environment, consumers store huge amounts of information (e.g. social networks, e-mail services…). At present, consumers are too often 'locked-in' to online services and platforms with no possibility of transferring this data onto other (competing) platforms. Existing terms and services appear to be mostly unfair in this regard: often service providers claim ownership of the data stored in their services.

This situation is incompatible with the right of consumers to be in control of their data and to object to the processing of their data. It also hinders competition among service providers and prevents switching. The right to data portability allows the consumer to be in control of his data and retain the ownership, by being able to shift the data to other services.

The relationship between the right to data portability and the right of erasure should be better clarified in the proposal. It should be clearly established that the right to data portability implies erasure of the data by the original service provider (the use of the word "copy" in Article 18.1 seems to imply that the original service provider can retain the data and only give away a copy). In any case the data controller is always obliged to delete the data when they are no longer necessary for the purpose for which they were processed (Article 5 [e]).

However, effective implementation of the right to data portability necessitates the development of interoperable or compatible standards.

Article 19 – Right to object

Article 19 of the proposal establishes the data subject's right to object to the processing of their data, unless the controller demonstrates compelling legitimate grounds for the processing. This is a significant improvement from the current situation, where the data subject only has a right to prevent processing where they can demonstrate damage is caused. According to Article 19, the data subject will have a default right to object to processing and it will be for the data controller to demonstrate why the objection is invalid and to justify the processing.

This provision however, does not make clear the consequences of the right to object in the relation to the data at stake. It should be clarified that the right to object, if upheld by the controller should result in the deletion of the data by the controller.

Moreover, the notion of "compelling legitimate grounds" which (despite the objection) could legitimise the process, should be clearly defined in the Regulation.

Article 20 - Measures based on profiling

Article 20 addresses the processing of personal data for the purposes of profiling individuals according to their personal aspects, preferences and behaviour. Advertising business models which use the profiles of individuals are proliferating and consumers are often unaware of these practices or the consequences in the economic decisions they take. Consumers have almost no control over the current complex "media and marketing ecosystem".

Therefore, BEUC welcomes the specific inclusion of profiling practices in the proposed regulation. BEUC is not opposed to the online profiling of consumers in principle. According to this logic, the draft Regulation does not prohibit profiling, but rather gives the consumer the right to object to profiling.

However, in order to ensure legal certainty it must be clarified what is meant by "legal effects" and "significantly affects". Moreover, the right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling in the advertising ecosystem; this obligation already exists in the current Directive and it should be reintroduced in the proposal. Equally, consumers should be informed of the possible consequences of profiling techniques applied to them.

The draft proposal should also prohibit profiling of vulnerable consumers such as children as those consumers often lack critical judgment and understanding of marketing techniques; those techniques could have a negative impact on children and young people's development.

Regarding paragraph 5, we do not support the reliance on delegated acts to specify the safeguards to protect consumers' legitimate interests in case of profiling. On the contrary, the safeguarding measures should be defined in the Regulation.

Article 21 - Restrictions

Article 21 of the proposal introduces a number of possible restrictions to the rights of data subjects. We note that this Article is much wider than the corresponding Article in the current Directive (Article 13). Contrary to the current Directive, the new Article 21 can be used to limit almost all the rights of the data subject (including the principles of processing, the right to object, measures based on profiling and the right to be notified of a data breach).

We believe that Article 21 should include certain guarantees in relation to the purposes, proportionality, necessity, categories of data processed and the persons authorised to do so. There is a need for more clarity on the specific guarantees that the law allowing such restrictions should establish in order to safeguard the legitimate interests of the data subject.

Under the current wording, Article 21 contains vague, undefined terms, such as "economic and financial interest", "monetary, budgetary and taxation matters" and even "market stability and integrity", the latter phrase having been added to Directive 95/46 without any further precision.

CHAPTER IV – Controller and processor

Article 22- Responsibility of the controller

The draft Regulation introduces the principle of accountability, according to which the data controller must put in place measures and control systems which ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.

Article 22 introduces a general obligation for the controller to implement appropriate measures and demonstrate compliance, while the following Articles of Chapter IV introduce further elements of accountability, including the carrying out of Data Protection Impact Assessments, the appointment of Data Protection Officers, the implementation of Data Protection by Design and by Default and the obligation to notify data breaches.

BEUC welcomes the new provisions enhancing controller's responsibilities which will help create a privacy and data protection culture within companies. They will also allow controllers to adopt the measures most appropriate for the nature of their processing operations, thus providing a high degree of flexibility as required by fast-evolving technology.

In addition to the requirement to demonstrate compliance to the DPA, it is equally important the controller demonstrates compliance to the public in general by means of an annual report describing the measures adopted.

The principle of accountability should not be perceived as an alternative to compliance with legal obligations or as an excuse to avoid administrative sanctions. The right to the protection of personal data is a fundamental right in Europe and its effective protection should not depend solely on the willingness of a company.

Strong enforcement and dissuasive sanctions are required when companies fail to comply with the law. It is however important to ensure that monetary fines do not become an objective per se in order to ensure the funding of DPAs, but should be proportionate to the infringement. When considering fines, the infringer should be given the opportunity to correct its behaviour.

Article 23 – Data protection by design and by default

BEUC welcomes the introduction of the principles of data protection by design and by default in the draft Regulation, making it compulsory for data controllers to implement appropriate measures to comply with them. These two principles will help empower data subjects' control and enhance enforcement of data protection legislation.

Article 23.1 establishes the principle of **data protection by design**, which would require privacy and data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal. BEUC welcomes flexibility provided to data controllers to comply with the general principles. BEUC would also welcome the inclusion of a reference to the use of Privacy Enhancing Technologies (PETs) as a tool to implement technical solutions to comply with the principle of data protection by design.

As regards the principle of **data protection by default,** BEUC believes that Article 23.2 should be revised to make it explicit that the privacy settings on services and products should by default comply with the general principles of data protection, such as data minimisation and purpose limitation. The data subject should have the choice to change the privacy settings and decide whether he wants to share his personal data and with whom. Privacy settings are an important aspect of online privacy. Consumers expect companies to create privacy settings that provide transparency and control over the ways in which organisations collect, use, and store personal information.

BEUC is also concerned that Article 23 only addresses the data controller. However, the processor should also be obliged to implement privacy by design and privacy by default while processing personal data on behalf of the controller. Such a requirement should be added in Article 26 which defines the obligations for data processors.

Article 24-Joint controllers

BEUC welcomes the provision on joint controllers (Article 24) and the introduction of an obligation to define their respective responsibilities for compliance with the obligations by means of an arrangement between them, while failure to comply with this obligation will entail administrative sanctions according to Article 79.5.e.

In practice, the chain of responsibility and liability is getting difficult to follow for data subjects not only as regards data controllers, but also controllers and processors (e.g. cloud computing), let alone that the distinction between data controller(s), data processor(s) and third parties is not obvious to the consumer. Although Article 26 requires the controller to define the respective responsibilities with data processor processing data on their behalf, BEUC recommends including a specific provision on joint responsibility between the controller and the processor, allowing the data subject to seek redress from each of them.

Article 25- representatives of controllers not established in the Union

BEUC welcomes the requirement for controllers not established within the EU to designate a representative to the Union. The representative is expected to be the contact point for both data protection authorities and the data subject. However, the broad exceptions to this obligation, including when the controller employs less than 250 employees cannot be justified. The exceptions must be fully justified or otherwise deleted.

Article 28- Documentation

Article 28 introduces the obligation for controllers and processors to maintain documentation of the processing operations instead of the cumbersome requirement for notification of the data controllers' personal data handling practices. Under the new Framework, data controllers should document any processing operation and be able to demonstrate compliance upon request to the Data Protection Authorities.

The documentation obligation, as defined in Article 28.2, includes the most relevant information and should not be simplified. The contact details of the controller and of the data protection officers, the types of personal data, the recipients of personal data, the purposes for processing, possible transfers to third countries and retention periods are the minimum information that any responsible and accountable organisation needs to keep records of. It will also make the checking by Data Protection Authorities easier and help improve monitoring of compliance and enforcement.

However, in order to comply with their obligations under Article 22, data controllers will in any case be able to demonstrate compliance with the legislation and the effectiveness of the undertaken measures. We would therefore support the proposal put forward by the European Data Protection Supervisor[6], to introduce an obligation to keep an inventory of all processing operations that would encompass general information, namely the contact details of the controllers (and joint controllers and processors if applicable), the contact details of the data protection officer and the description of the mechanisms implemented to ensure the verification of the measures undertaken in order to ensure compliance. More specific information should be part of an additional obligation to inform data protection authorities upon request.

As regards the exception from the documentation obligation for organisations with less than 250 employees, BEUC would suggest its deletion or its replacement with a criterion based on the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data on. The exception should only apply to those entities that are processing data as an accessory activity.

Article 31-32- Notification of a personal data breach authority

BEUC welcomes the introduction of a horizontal data breach notification obligation for the controller, beyond the telecommunications sector. Consumers may suffer at least the same harm from the undue disclosure of their bank account details as from the disclosure of their telephone bills.

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

The draft Regulation introduces a dual system of notification, according to which all breaches must be notified to the Data Protection Authorities (Article 31), while only those breaches that adversely affect the protection of personal data and privacy should be notified to the individuals (Article 32).

BEUC agrees that only those breaches that adversely affect the individual should be notified to data subjects. A general obligation to notify individuals whenever personal data has been compromised might be counter-productive and lead to "notification fatigue" and de-sensitisation.

[6] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.

However, the definition of what constitutes a breach of adverse effect is only partly provided in Recital 67. In order to ensure legal certainty and a consistent approach across Europe, BEUC would suggest including the definition in Article 32. Such a definition should be broad and encompass not only those breaches which result in economic loss, but also breaches which may cause immaterial damages, such as any moral and reputational damages. Additional criteria, such as time spent in attempts to rectify the breach and distress should also be considered when assessing the adverse effect.

BEUC supports a risk-based definition of the adverse effect of data breaches. In order to determine the level of risk, both quantitative and qualitative indicators need to be considered. For example, the type of data, the number of individuals affected and the amount of data breached would have to be considered.

As regards the content of the notification, the requirements set in Article 32.2 should also comprise a description of the consequences of the personal data breach (Article 31.3[d]); in addition, the individual should be informed about their rights and be provided with the contact details of the Data Protection Authority and consumer associations who can help them seek redress.

BEUC also suggests including a specific requirement for the notification to be clear and comprehensive, i.e. without technical jargon. It should be sufficient for the individual to read the notice in order to understand the risks and recommended actions.

BEUC regrets the fact that only the data controller is required to notify breaches. This obligation should also cover breaches occurring while personal data is being processed by the data processor. In this case, the data controller should bear the responsibility to notify.

As regards the notification to the data protection authorities, BEUC believes that the notification must take place as soon as possible, without undue delay and not beyond 72 hours after the controller becomes aware of the data breach.

We would also suggest that a specific deadline is introduced for the DPA to act on a breach notification, as well as a deadline within which the data controller should notify the breach to the data subject.

Articles 33-34 – Data Protection Impact Assessment and prior authorisation

BEUC welcomes the introduction in the EU Data Protection framework of an obligation for the controller and the processor to carry out an assessment of the impact on the protection of personal data of the processing operations that present specific risks. The implementation of meaningful PIAs complying with high privacy standards also figures in the Madrid Privacy Declaration adopted by the International Conference of Privacy and Data Protection Commissioners in November 2009.

A robust framework of Data Protection Impact Assessments can be an effective tool to address the challenges of a fast evolving ICT sector and help identify the risks to consumers' fundamental rights to privacy and to protection of personal data at an early stage. As such, a DPIA is an integral part of the privacy by design principle. It also enables data controllers and processors to demonstrate compliance with the requirements of the Regulation.

A DPIA should also be carried out when processing operations "are likely" to present specific risks to the rights and freedoms of data subjects[7]

We are also concerned with the limitation of processing operations to processing on a large scale when information about the sex life, health, race and ethnic origin or for the provision of healthcare etc. (Article 33.2.[b]). This type of information is sensitive personal data and therefore a PIA should be mandatory irrespective of the scale of processing.

BEUC also suggests introducing in Article 30 a specific requirement for the DPIA to be made publicly available, or at least a summary of it. It should be for the national Data Protection Authorities to maintain a registry of PIAs, similar to the system in the District of Columbia in Canada[8]. This would allow individuals to consult the PIAs and increase their confidence in handling of their personal data. It goes without saying that the PIAs or their summaries should be published in a reader-friendly format.

BEUC would support the audit of DPIAs by the Data Protection Authorities to ensure it fulfils the conditions set out in the Regulation. This would increase the reliability of DPIAs and would also facilitate the establishment of a central registry open to consultation by all stakeholders.

Articles 35-37- Data Protection Officer

BEUC welcomes the introduction of the obligation for both controller and processor to appoint a Data Protection Officer (DPO) within the framework of the accountability principle. DPOs are familiar with the problems and the processing activities of the entity they work for and can therefore provide valuable advice as to implementation of the Regulation and monitor compliance. It is also expected that the appointment of a DPO will help increase awareness of data protection rules within the entity; according to a Eurobarometer (2008) survey, only 13% of people responsible for data protection within companies said that they were very familiar with the provisions of data protection law[9].

[7] This will also align the wording of Article 33.1 with the wording in Articles 34.2(a) and 33.6.
[8] PIAF, Privacy Impact Assessment Framework for data protection and privacy rights, Deliverable 1 http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf
[9] Eurobarometer survey on data protection in the EU, February 2008.

The appointment of a DPO should be mandatory, except for those entities processing personal data as an accessory activity. The proposed threshold of 250 employees for requiring the designation is unjustified, given that all Small and Medium Enterprises would escape this obligation. BEUC counters that the determining factor should not be the number of employees, but the nature of the processing activities, the volume and the type of personal data involved and the number of data subjects the enterprise processes the data of.

DPOs must have expert knowledge of data protection law and sufficient experience to carry out the assigned tasks. Given their special role, there must be mechanisms in place to check and verify the qualification of DPAs. This will also be to the benefit of data controllers, who risk administrative sanctions for failing to appoint a DPO or for not respecting the conditions for its appointment, according to Article 79.6.[j]. DPAs could also organise regular training seminars for appointed DPOs.

The draft Regulation requires DPOs to be independent from the data controller or processor. However, in practice there will most often be an employment relationship between the two parties. Therefore, BEUC would suggest further strengthening the independence of DPOs by requiring the controller or processor to submit a fully justified report to a DPA in instances of the dismissal of a DPO (Article 35.7). In addition, in instances of disagreement between the DPO and the controller or processor, or doubt as to compliance with rules, it should be for the supervisory DPA to provide guidance.

Articles 38-39– Codes of conduct and certification

BEUC is concerned by the encouragement of codes of conduct to be developed by controllers and processors. Self-regulatory codes can only be endorsed if they entail an added value for consumers' rights by offering a higher level of protection, are backed up by suitably robust auditing or testing procedures and provide for independent complaint handling and enforcement mechanisms.

However, Article 38 does not address these concerns. On the contrary, it only provides for the possibility for industry associations to submit the draft codes to supervisory authorities, which can only issue a non-binding opinion. Furthermore, the draft Regulation is rather weak when it comes to complaint handling mechanisms, the development of which is left exclusively to data controllers and processors. Similar inter-company complaint handling schemes should by no means be recognised as out of court dispute resolution procedures as they lack independence.

The development of EU certification schemes and privacy seals could become an effective means of ensuring 'privacy compliant' or even 'privacy enhancing' IT products, websites, companies 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 and quicker choice. However, it is important to clarify that the granting of a seal would not simply certify compliance with the law, but provide an added layer of protection.

BEUC supports 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. 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.

It is therefore regrettable that the Commission has reserved the right to specify by way of delegated acts the criteria and requirements, including the conditions for granting and withdrawal. It would be preferable if more substantive rules are included in Article 39 to ensure legal certainty.

CHAPTER V – Transfer of personal data to third countries or international organisations (Articles 40-45)

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. The draft Regulation recognises the new reality and abandons the presumption that personal data may not be transferred without an adequacy level of protection, setting instead a number of principles which must be fulfilled when personal data is transferred outside the EU.

BEUC welcomes the inclusion among the factors to be considered when assessing the **adequacy** of , elements related to the rule of law, the existence of effective and enforceable rights as well as means of redress for data subjects (Article 41.2.[a]). It is also positive that the adequacy recognition will also depend on the international commitments of the third country, which would also include ratification of the Council of Europe Convention.

In the absence of an adequacy decision, the draft Regulation allows for the transfer of data provided that the controller and/or the processor have adduced appropriate safeguards in a legally binding instrument. Such safeguards will be provided by Binding Corporate Rules (BCRs), standard data protection clauses approved by the Commission or adopted by a DPA.

BEUC regrets that the proposal opens the possibility for transfer when safeguards are not provided in a legally binding instrument (Article 42.5), which might urge controllers to adopt codes of conduct. A similar derogation cannot be justified and therefore it should either be deleted or limited to a few specific cases.

Transfers should not be possible for those countries for which the European Commission has already adopted a decision not recognising the adequacy of their status.

Binding Corporate Rules have already been endorsed by the Article 29 Data Protection Working Party and therefore their explicit recognition as an adequate mechanism for transfer of data to third countries in Article 43 is welcome. It is important that BCRs are binding and enforceable upon all members of the controller and processor's undertakings and that implementation will require approval by the supervisory authority.

BEUC is concerned with the broad scope of Article 44 on **derogations**. It should be made explicit that derogations can only apply to a restricted number of cases of occasional transfer that cannot be qualified as frequent, massive or structural, as pointed out by Article 29 Data Protection Working Party[10] and the European Data Protection Supervisor.

Furthermore, the consent of the data subject can be used as derogation to the rules on international transfers. As already outlined, it is questionable whether the data subject has the sufficient knowledge to fully assess the implications of any transfer of their personal data to a third country without an adequate level of protection and with no safeguards from the controller. Article 44.1 should therefore be deleted.

We are also concerned with the broad definition of the "public interest" which would also cover the transfer of personal data to third countries for the prevention, investigation, detection and prosecution of criminal offences (Recital 87). A similar provision would increase the risk of abusive transfers to law enforcement authorities without any safeguard for the protection of data subjects' fundamental rights.

As regards **international cooperation** on the protection of personal data, Article 45 aims for enhanced cooperation between data protection authorities in **enforcing the law.** Although such cooperation is crucial, we are concerned by the role envisaged for stakeholders in enforcing the law. Such a provision relates to the recently announced Consumer Privacy Bill of Rights in the USA which foresees the development of codes of conduct as a tool to enforce the law. BEUC is concerned that such schemes of self and/or co-regulation fail to provide a robust enforcement system.

Lastly, BEUC regrets the deletion during the inter-service consultation of a provision that would have prohibited the transfer of personal data based on **orders or requests from non-EU courts, tribunals, administrative authorities and other governmental entities**. It stated that in cases where a third country requests the disclosure of personal data, the controller or processor had to obtain prior authorisation for the transfer from its local supervisory authority. This provision is particularly relevant with regards to requirements under US law for the disclosure of data, in particular based on law enforcement requirements or e-discovery requests. The US uses instruments such as the Foreign Intelligence Surveillance Act (FISA) and the Patriot Act to retrieve data on the political activities of foreign individuals who may have no links whatsoever to the USA, via companies with US offices. We would suggest that this provision is added in a separate, new Article.

[10] Working document of the Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26.1 of Directive 95/46 of 24 October 1995 (WP114).

CHAPTER VI – Independent Supervisory Authorities (Articles 46-54)

BEUC welcomes the provisions of the draft Regulation which establish explicitly the **independent** status of Data Protection Authorities in order to ensure the effectiveness and reliability of the supervision of compliance with the legal framework.

However, we regret the absence of specific standards for the **funding** of the operations of Data Protection Authorities. Article 47.5 only calls upon Member States to ensure that DPAs are provided with adequate human, technical and financial resources[11]. Adequate funding is a key element to ensure the independence of DPAs. Such funding should be proportionate to the number of data controllers DPAs regulate and the individuals whose personal data is processed.

We therefore suggest that specific provisions are added in Article 47 which would outline complementary sources of funding for DPAs. In its document 'The future of privacy', the Article 29 Data Protection Working Party suggested alternative sources of **funding**, which may range from a fully fee-based model (based e.g. on notification fees and the levying of fines for breaches of the law) to a fully state-funded model[12]. We would also like to underline that, in many cases, DPAs may be reluctant to impose sanctions against companies due to the increased costs of counter-litigation if companies challenge the sanctions imposed. This may undermine the capacity of DPAs to undertake action.

As regards the provisions on the competence of DPAs and the introduction of a "**one stop shop**" for data controllers or processors, BEUC is concerned that **Article 51** might result in **forum shopping**. It should be made explicit that the powers of the lead authority are not exclusive and that coordination between all relevant DPAs is ensured. Otherwise, there is a significant risk that the data controller will decide to establish itself in those Member States with less stringent rules, as a degree of flexibility on the applicable law would still be left to Member States.

There should also be a clear definition of the main establishment. As previously stressed, the definition provided in Article 4 is inappropriate for undertakings with a decentralised decision making structure, where the central administration and location of management decisions about data processing differ. It would be more appropriate to introduce a number of specific factors/criteria needed to be considered to assess the lead authority, such as the number of data subjects whose personal data is affected.

[11] See also Article 29 Data Protection Working Party letter to Vice-President Reding. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120404_letter_to_vp_reding_resources_en.pdf

[12] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf.

Furthermore, the rules on the lead authority will only apply where the controller has an establishment in the European Union. **Article 51 does not cover those cases where there is no establishment in the EU**, in cases where the processing activities are related to the offering of goods and services to data subjects residing in the Union or the monitoring of their behaviour. Given that similar processing activities may easily affect data subjects in multiple EU Member States, specific rules on the assignment of a lead authority should also be defined. BEUC believes the lead authority should be that of the Member State where most data subjects have been affected, or the Member State where a specific complaint has been lodged.

A key issue which is left unaddressed in the draft proposal is who should be responsible for the appointment of the lead authority (the authority or the controller) and how disputes regarding appointment of the lead authority are to be solved.

Article 52 provides for the duties of supervisory authorities, including the power to hear **complaints lodged by data subjects** (52.1.[b]). Given that the lead authority might be different from the one of the residence of the data subject, a number of practical problems need to be solved, including who bears the costs for translation and/or interpretation. These should not be borne by the data subject, as it would be a major obstacle to the exercise of his fundamental right to redress.

CHAPTER VII – Cooperation and consistency (Articles 55-72)

BEUC welcomes the focus of the draft Regulation on enhancing **cooperation and coordination** between Data Protection Authorities. Article 56 empowers DPAs to undertake joint operations, including joint investigations and joint enforcement measures. Article 55.2 introduces the duty to take action upon request of another DPA within one month. Failing to comply with this duty, the DPAs may take provisional enforcement or compliance actions in another Member State. Nevertheless, we are concerned about the nature and the scope of similar measures since it might raise problems of interference with national procedural and constitutional law.

Strengthening the cooperation between DPAs is crucial, given that a data breach may well affect data subjects across Europe and beyond. However, this should not be the only mechanism for ensuring cross-border enforcement of data protection laws. To this end, the experience with the Consumer Protection Cooperation Regulation needs to be assessed. A number of interesting conclusions can be derived from the most recent report on the implementation of the CPC Regulation published in March 2012. Despite the fact that the CPC network has already been established for several years (since 2006), there is still no uniform understanding among the national authorities about how to use the cooperation tools. Furthermore, the average time for the handling of mutual assistance requests is 92 days. Article 55.2 of the draft Regulation requests DPAs to act within 30 days[13].

[13] http://ec.europa.eu/consumers/enforcement/docs/comm_biennial_report_2011_en.pdf

With regards the "**consistency**" mechanism, BEUC sees the merits of the need for a more coherent approach of DPAs to issues of common interest. However, we are concerned that in almost every case when a DPA considers the adoption of measures against a company operating internationally, it will trigger the consistency mechanism. There needs to be a threshold in the draft Regulation to ensure consistency only applies to processing that raises serious risks to data subjects across Europe.

Furthermore, the draft Regulation allows the European Commission to intervene extensively in the context of the consistency mechanism. In particular, the Commission can ask for the consistency mechanisms to be applied, but can also suspend a measure adopted by a DPA if there are serious doubts as to its effectiveness (Article 60). BEUC agrees with the European Data Protection Supervisor to limit the suspension to cases where there is, *prima facie, a* clear breach of EU law subject to scrutiny of the Court of Justice[14]. The same concerns are raised by the power of the European Commission to overrule a decision of a national DPA via an implementing act (Article 50.1 and 62.1.[a]).

The provisions of the draft Regulation may undermine the independence of DPAs and subject their decisions to the external influence of the European Commission. The Commission could adopt its own Opinion but without any effect on the decision of the European Data Protection Board, while in cases of serious conflict it should be for the European Court of Justice to decide.

Lastly, BEUC welcomes the provisions on the establishment of the **European Data Protection Board** to replace the Article 29 Data Protection Working Group, particularly with regards to its independence. The status and the legal nature of the Opinions of the Board are necessary to ensure they become binding particularly when they concern the interpretation of provisions of the Regulation.

CHAPTER VIII – Remedies, liabilities and sanctions (Articles 73-79)

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 of the competent forum and applicable law, act as a deterrent in the enforcement of data subjects' rights and an impediment to the fundamental right of access to justice.

BEUC welcomes the introduction of provisions which provide for **several redress mechanism**s with the view to facilitate enforcement by the data subject (Article 73). It is important that individuals can choose to lodge a **complaint with any DPA**, mainly that of their country of residence. However, it must be clarified that any costs related to the translation or transfer of the complaint to the competent

[14] Opinion of the European Data Protection Supervisor on the data protection package reform, 7 March 2012.

DPA of another Member State should not be borne by the data subject.

As regards the right to a **judicial remedy** against the controller and the processor, BEUC welcomes the provision enabling the individual to lodge the complaint either before the court of the country of establishment of the controller or the court of the residence of the data subject. In cases where individuals from different countries have lodged complaints in different jurisdictions, the complexity can be solved through the establishment of clear rules regarding the competence of courts. For instance, it can be clarified that the court of the place of the most affected data subjects is the competent one and the others should suspend proceedings until the ruling is issued. However it should be ensured that the ruling can be recognised and executed in all other Member States.

Despite our support for the proposed redress mechanisms, we believe that in addition, more cost and time efficient methods for consumers to enforce their rights should be considered.

BEUC welcomes the right of organisations **or associations defending data subjects' rights** to lodge a complaint before a supervisory authority (Article 73) or bring an action to court (Article 76) on behalf of data subjects. However, we regret that the proposal has stopped short of introducing fully fledged **collective judicial actions** whereby representative bodies can claim compensation for the damages suffered by data subjects.

BEUC supports a system of collective judicial actions on the basis of Europe's legal tradition and the experiences of EU Member States. A number of safeguards need to be included to ensure such a system is not abused. BEUC has developed ten golden rules for a European, judicial, collective action[15] which addresses the risk of abuse and provides a cost-effective and fair mechanism.

BEUC calls for a specific provision to be included in Article 77 which allows a representative organisation to bring judicial actions for compensation. There should be a clarification as regards the **quantification of damages and the calculation of compensation**. To this end, the possibility for **flat rate compensation** to be provided in circumstances of data breaches should be considered. 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 and consequently so is the illegal benefit of the non-compliant company.

An illegal behaviour of abuse of personal data can easily affect a high number of people, especially in the online environment, where internet 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 involved parties, while in some cases, there might be no immediate damages, such as when confidential data (credit card numbers) are leaked.

[15] European Group Action, BEUC's ten golden rules
http://docshare.beuc.org/docs/2/MMOLGAFDFOMBPINPIJPPOEMDPDBW9DB67K9DW3571KM/BEUC/docs/DLS/2008-00394-01-E.pdf

It should also be clarified that consumer organisations are entitled to bring actions for breaches of data protection law. In some EU Member States, consumer organisations can only act for breaches of consumer protection legislation, and data protection falls outside their remit. Nevertheless, consumer associations are credible entities with long experience in defending consumers and should therefore be entitled to act in the field of data protection. It should also be clarified that **damages** should include not only material and quantifiable damages, but also immaterial damages and distress. It is also important that consumer associations have standing to represent also consumers from other Member States that have suffered damage from the same illegal behaviour.

BEUC also welcomes the **joint liability** of the data controller and data processor, particularly as it may be difficult for the data subject to determine which entity is the data controller and who bears the liability in cases of damages suffered.

Article 79 aims to strengthen the mechanisms for **sanctions** in case of data protection infringements. The sanctions foreseen resemble the ones established under competition law and aim to act as a major deterrent for companies involved in the processing of personal data. However, BEUC proposes that the fines imposed on companies could be used, at least in part, to finance the actions of organisations defending the rights of data subjects. Furthermore, safeguards need to be included if fines are to be used mainly for the funding of DPAs to ensure that the system is not abused.

As regards the **exceptions** foreseen for processing by natural persons without commercial benefit and for entities below 250 employees for which personal data processing is an activity ancillary to its main activities, BEUC believes the important factor should not be the number of employees, but rather on the nature of the activities. For example, consumer organisations may well carry out surveys with the aim of advising consumers that might involve the processing of personal data. Such an activity is ancillary to the normal activities of consumer organisations and should therefore be exempted from the scope of Article 79.

CHAPTER IX – Provisions relating to specific data processing situations (Articles 80-85)

Chapter IX leaves room for national rules for specific processing situations related to freedom of expression, health, employment, professional secrecy, churches and religious associations.

Article 80: Processing of personal data and freedom of expression

BEUC welcomes the exemption from the regulation when personal data is carried out for journalistic purposes or for the purpose of artistic and literary expression. The freedom of expression must be balanced with the right to protection of personal data to ensure the effective exercise of both. To this end, an assessment on a case by case basis may be required to ensure that the right to data protection is not misused to hinder freedom of expression and freedom of information.

We would also suggest that the notion of journalistic purposes is clarified to include not only the traditional media, but also all new activities whose object is the public disclosure of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper, radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities, in line with the rulings of the European Court of Justice[16].

Article 81- Processing of personal data concerning health

Article 81 foresees a number of exceptions to the general prohibition of processing sensitive health data: we support those exceptions as they ensure a good balance between the right to privacy, consumer safety and public health interests, but we think that certain aspects should be further clarified to prevent abuses. Moreover the use of sensitive health data for marketing purposes should remain prohibited. Tracking and profiling technologies in health related websites should not be allowed.

Article 81 allows the use of compiled health data for research purposes, for better managing healthcare expenditures, for monitoring and improving the quality, safety and the effectiveness of medicines and medical devices. Whilst we do not question the benefit of this for the safety of the individuals and for public health, we question the actual possibility of ensuring the anonymity of data. Technological advances in data analysis and combination with other data sets could endanger anonymity and lead to the identification of individuals. Unanswered questions remain also as to who exactly would have access to such data. For example, would the research sector include pharmaceutical companies? Would public accessibility mean that insurers can access the data? The legislation also lacks an indication as to how the amount of information seen will differ according to the role of the person accessing it. For example, how will the data which patients see differ from the data available to healthcare staff, policy makers and third party researchers?

It is crucial that only authorised and specifically trained healthcare professionals have access to patients' health records. Article 81 mentions the processing of data could be done by a person other than the healthcare professional provided that they are subject to an equivalent obligation of confidentiality. The definition of another person should be further specified to prevent abuses and inconsistency with the other provisions of the legislation.

[16] C-73/07- *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*.

Article 83- processing for historical, statistical and scientific research purposes

BEUC welcomes the exemption when personal data is processed for historical, statistical and scientific purposes. It should however, be stressed that the preferred option should be the processing of anonymised data and that only when it is impossible for the specific research, personal data should be processed when the conditions of Article 83 are met.

CHAPTER X – Delegated acts and implementing acts (Articles 86-87)

The draft Regulation often empowers the European Commission to adopt delegated and implementing acts. Although such acts can in certain cases ensure a uniform implementation of the Regulation, BEUC is concerned that the extensive use of this mechanism, as foreseen by the proposal, will undermine the objective of establishing a clear and comprehensive set of rules to the detriment of both data subjects and businesses. We are also concerned about the time required for all delegated acts to be issued: according to the estimated financial impact statement accompanying the Regulation proposal, only two delegated acts will be administered per year, and therefore a period of ten years will be required to adopt all acts and achieve legal certainty.

Furthermore, we are concerned with the lack of democratic oversight in the adoption of delegated and implementing acts; all EU institutions should have be involved.

BEUC suggests that the number of provisions subject to the adoption of delegated and implementing acts should be significantly reduced and limited to those provisions addressing non-essential issues, such as design requirements, criteria for technical measures etc. Furthermore, the mechanism of Article 86 could be used as the basis to adopt sector-specific rules clarifying the application of the general framework to specific areas of law. We would therefore suggest the possibility for the adoption of delegated acts and implemented acts is **maintained** only for the following provisions:

- Article 8.3 referring to the definition of criteria and requirements to verify parental consent in case of processing of personal data of a child below the age of 13 years old;
- Article 14.7 with regards to the modalities for the provision of information to the data subject;
- Article 15.3 on the content of the communication to the data subject of the personal data undergoing processing following a request to access data;
- Article 22.4 on the appropriate measures to be adopted by the data controller to ensure compliance in accordance with the principle of accountability which requires a certain degree of flexibility;
- Article 23.3 on the design requirements for the application principle of data protection by design on specific products and sectors;

- Article 26.5 regarding the measures to be adopted by the data processor in order to comply with the obligations established in the Regulation;
- Article 28.5 on definition of criteria and requirements for the documentation obligation;
- Article 30.3 which deals with technical aspects of security;
- Article 35.11 on the qualification of the data protection officer;
- Article 37.2 regarding the tasks, certification, status, powers and resources of the data protection officer;
- Article 43.3 on further specifying the criteria and requirements of binding corporate rules;
- Article 79.6 on the update of the amounts of the administrative fines.

As regards the remainder of the cases, it is crucial that further clarification is included in the current Regulation, as they refer to substantive and essential elements and therefore call for legal certainty. This is the case with the following provisions:

- Article 6.5 which foresees the adoption of sector-specific rules clarifying the application of the legitimate interests of the data controller as grounds for lawful processing; there is the risk that unless clearly specified, the legitimate interests of the controller may be invoked by controller to legitimise processing even when there is no appropriate legal grounds;
- Article 9.3 referring to sensitive data; the processing of sensitive data requires an additional layer of protection due to the nature of the information they can reveal about an individual and therefore the conditions and the safeguards for their processing must be clearly defined in the draft Regulation. Alternatively, this could be the object of opinions or reports of the European Data Protection Board;
- Article 12.4 regarding the definition of threshold above which requests to access and correct one's own data will be considered excessive. Otherwise, there is a risk that Member States use different thresholds and thus hinder the effective exercise of the individual rights;
- Article 17.9 on the implementation of the right to be forgotten. Given the interaction with fundamental freedoms, the conditions for deleting links, copies from publicly available communication services should be defined upfront;
- Article 18 regarding the right to data portability, the effective implementation of which requires the development of interoperable or compatible standards;
- Article 20.5 reserving the right for the Commission to define the safeguards for the data subject when profiling is allowed. This provision touches upon essential and substantive elements of data subjects' protection;
- Article 31.5 which refers to the threshold for data breach notification; unless a threshold is clearly defined in the Regulation, all breaches might have to be notified to the data protection authority;

- Article 32.5 on the communication of a data breach to the data subject. It is crucial to define when a breach will seriously affect the rights of the individual and will therefore require notification;
- Article 33.6 regarding the definition of operations presenting specific risks and therefore subject to a data protection impact assessment;
- Article 34.8 on the definition of the high degree of specific risk demonstrated by an impact assessment;
- Article 39.2 on certification mechanisms and privacy seals. For certification and seals to be endorsed by data subjects, full compliance with the legal framework and high standards of protection need to be ensured. It is therefore important that the conditions for the granting and the recognition within the EU are clearly defined;
- Article 44.7 on the notion of the public interest that might justify a derogation from the rules on transfer to third countries;
- Article 81.3 on the notion of public interest in relation with the processing of personal data concerning health;
- Article 83.3 regarding the criteria for limiting data subjects' rights for the processing of historical, statistical and scientific research purposes.

END