The Consumer Voice in Europe

Proposal for a Data Protection Regulation

BEUC analysis of consumer benefits versus administrative burden of key provisions

REF: BEUC-X-2014-088 - CONTACT: digital@beuc.eu

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 • www.twitter.com/beuctweet • www.beuc50years.eu
TVA: BE 0422 071 051 • EC register for interest representatives: identification number 9505781573-45

BEUC welcomes the proposal for a Regulation on Data Protection as a major improvement for individuals, particularly in light of the ever-increasing use of personal data in the internet environment. The proposal strikes the right balance between, on one hand the need for an effective system of data protection, and on the other for businesses not to be confronted with excessive administrative burdens.

And yet, lesser administrative burden should not result in weaker protection of personal data nor limit the liability of companies *vis-à-vis* data subjects. On this theme, the draft regulation has abolished the burdensome notification procedure while establishing the principle of accountability according to which the data controller will adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the Regulation.

The new provisions will allow controllers to adopt the measures most appropriate to the nature of their activities, thus providing a high degree of flexibility. In parallel, the proposal will help restore consumer control over personal data and enhance consumer trust. Therefore BEUC urges you not to overestimate the impact on businesses, but instead ensure the adoption of a user-centric approach by placing the data subject at the forefront of your considerations.

Consumer confidence is essential to economic recovery. According to the Eurobarometer survey (No. 390), a lack of consumer trust acts as a significant barrier to the development of e- commerce and the digital economy. A solid framework for data protection would help boost consumer confidence, especially in the complex online environment. Innovation will only be able to be rolled out on a large scale if people trust the way their data is being handled.

The present paper has looked at a set of provisions in the draft Regulation, providing a comparative assessment of the impact on the protection of individuals' personal data and the impact on businesses. It becomes obvious that businesses will benefit significantly from the new rules, both in terms of legal harmonisation and reduction of administrative burden.

If further action is deemed necessary to mitigate the risk of legal uncertainty and administrative burden, this should focus on minimising the provisions subject to the adoption of delegated and implementing acts, thus allowing data controllers more flexibility in the choice of measures and subject to guidance by the European Data Protection Board.

-Overall assessment-	
Impact on consumers	**Impact on businesses**
Strengthening and clarification of key data protection principles, including data minimisation and purpose limitation. Strengthening of the rights of data subjects to access their data. More transparency about how your data is handled, with easy-to-understand information, putting an end to privacy notices full of legal jargon. Notification about breaches of their personal data without undue delay. Improved administrative and judicial remedies in cases of violation of data protection rights. Increased responsibility and accountability for those processing personal data – including through the principles of 'privacy by design' and 'privacy by default'.	A level playing field for businesses through one single law applicable to any business across the EU. This harmonisation is expected to save businesses up to €2.3 billion per year. A 'one-stop-shop' – companies in the EU will be answerable to a single data protection authority (DPA), no matter how many EU countries they do business in. Abolition of the current obligation to notify data processing, which costs businesses about €130 million per year. The accountability principle grants business es the flexibility to adopt appropriate measures in order to comply with the obligations set by the draft Regulation (Article 22).

Right of access	
Article 15 ***"The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information."***	
Impact on consumers	**Impact on businesses**
The proposal deletes the possibility for data controllers to charge consumers a fee for accessing their personal data that has been processed. The right of (free) access of data subjects to their personal data underpins the right to retain the ownership and the control of the data by the data subject at all times. Consumers have a right to know what data a company or organisation holds about them and should not have to pay to access their personal data. In a survey commissioned by the UK consumer organisation Which? 76% of consumers said that they found it unacceptable or completely unacceptable that companies can charge £10 to provide the information held about them.	Businesses claim that the obligation to give free access will lead to unscrupulous requests to access that would be costly for them. The Commission's proposal already includes an exception for requests which are manifestly excessive, in particular because of their repetitive character. However there is no valid reason or data that demonstrates that this would be the case. For instance, in those countries where the fee has been abolished, this did <u>not</u> result in any increase of requests.

Data portability	
Article 18 ***"The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject."***	
Impact on consumers	**Impact on businesses**
The right to Data Portability will ensure consumers are not 'locked in' to services and are able to easily retrieve their data and change provider. The right to data portability will enable people to recover and/or to shift their own data from one platform/cloud to another. However, for this right to be effective, interoperability between services and promotion of open standards is required.	An effective right to data portability will help promote competition. It will help reduce monopolisations of market power and improve competition in the market, so that new services can innovate and attract consumers away from the original service. The right to data portability already exists under EU law, including number portability for telecommunications operators.

Responsibility of the data controller
Article 22   ***"The <u>controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate</u> that the processing of personal data is performed in compliance with this Regulation.***   ***"The <u>controller shall implement mechanisms to ensure the verification of the effectiveness of the measures</u> referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors."***

Impact on consumers	**Impact on businesses**
Accountability shifts the primary responsibility for data protection from the individual to the organisation collecting and using data. Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing the marketplace for enterprises using data irresponsibly. The new Regulation will enhance data protection efficiency by allowing regulators to focus their resources on activities which pose the greatest risk to individuals.	Only the abolition of the notification requirement saves businesses €130 million per year. The average cost for each notification is estimated to be €200. Businesses will enjoy sufficient flexibility in the choice of the means to adopt in order to comply with the obligations set in the Regulation. Businesses will be able to more effectively conserve scarce resources allocated to data protection. Accountability directs scarce resources towards mechanisms which most effectively provide protection for data. Organisations will adopt the tools best suited to guaranteeing protections focus on reaching substantive privacy outcomes (measurable information protection goals) and to demonstrate their ability to achieve them.

Data Protection by Design ***Article 23:*** ***"The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."***	
Impact on consumers	**Impact on businesses**
Data Protection by Design will help limit the collection of personal data and consumers trust that their personal data is protected. Data Protection by Default will ensure that even non-digital consumers, who are unfamiliar with privacy settings of services and products will have protection. These two principles will help empower data subjects' control and enhance enforcement of data protection legislation. Consumers' personal data will be respected throughout the lifecycle of products and services.	Organisations who collect, use and disclose personal information should proactively accommodate the privacy interests and rights of individuals throughout their operations. The "payoff" to organisations would come in many ways, including: improved customer satisfaction and trust; enhanced reputation; commercial and enduring competitive advantage. 77% of the security industry believes that it should be a mandatory obligation. More than 13 EU projects related to privacy enabling technologies are currently funded by the EU budget. An additional call for projects related to security and privacy has been published in July 2011 with a budget of €80 million. These measures would provide support to the application of the principle of Privacy by Design in the industry. Privacy by Design rules are already included in the national legislation of many EU Member States.

Article 28 Documentation	
Impact on consumers	**Impact on businesses**
The documentation obligations will facilitate the task of Data Protection Authorities when monitoring the compliance of data processing operations with the principles and rules set in the Regulation. The documentation obligations will facilitate the enforcement of the Regulation by both data subjects and the data protection authorities.	The obligation to maintain documentation about the processing operations partly replaces the cumbersome notification obligation. The current obligation to notify data processing costs businesses approximately €130 million per year. The documentation items in Article 28 refer mostly to the information that the consumer should receive when their data is processed and therefore the extra burden from the documentation obligation is zero. The documentation obligations refer to the minimum information that any responsible and accountable business needs to keep records of in particular in the context of the obligation to carry out an impact assessment.

Data Breach Notification Obligation	
Article 31: ***"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours."*** ***Article 32:*** ***"When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay."***	
Impact on consumers	**Impact on businesses**
Data breaches can lead to significant harm to consumers, ranging from undesired spam to identity theft. 88% of Europeans want to be informed when their personal data is lost, stolen or compromised (Eurobarometer). 74% of UK consumers would always wish to be notified of a data breach (Which? survey). A data breach notification will also include information about measures to be taken by the individual in order to mitigate the impact of the breach.	The cost will be minimal: according to the Impact Assessment of the European Commission 7. 1% of EU companies have experienced a breach, of which: - 55% actually informed the individual whose data was affected and - indicated a cost of less than €500 for the notification.

Data Protection Impact Assessment

Article 33

"Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

Impact on consumers	**Impact on businesses**
Consumers can trust that a business has implemented a thorough assessment of the potential risks related to the protection of personal data and has taken measures to mitigate them. Consumers have the opportunity to provide their views within the framework of the DPIA. A DPIA provides consumers with enhanced transparency on the processing operations carried out by businesses.	A DPIA is an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments. A DPIA enables an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation. A company that undertakes a DPIA and engages with data subjects and their representatives will earn trust from consumers and maintain a competitive advantage over competitors. If an organisation has engaged with stakeholders from an early stage, it will be very difficult for stakeholders to claim negligibility of the business at a later stage.