PRIVACY INTERNATIONAL

Summary analysis of European Commission proposal for a general Data Protection Regulation

Privacy International
46 Bedford Row
London WC1R 4LR
Phone +44 (0)20 7242 2836
info@privacy.org
www.privacyinternational.org
Twitter @privacyint

September 19 2012

On 25 January 2012, the European Commission published a proposal that would comprehensively reform the European data protection legal regime. One aspect of its proposal, a new Regulation (the "Proposed Regulation"),[1] would modernise and further harmonise the data protection regime created by the Data Protection Directive (95/46/EC). Another aspect of the Commission's proposal, a new Directive[2] (the "Proposed Directive"), would set out new rules on "the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data"[3].

As regards the proposed Regulation, we believe that on the whole it goes a long way towards ensuring that data protection law is capable of adequately responding to contemporary and emerging threats to the right to privacy. Importantly it goes some way towards ensuring that all citizens of EU member states will have equal access to these protections. It starts from the standards and principles set out in the current Directive (95/46/EC) and further enhances, elaborates and develops these. As a result it ensures more control on the part of the individual citizen/consumer for example with regards to access, correction and deletion and by attempting to ensure that these rights are meaningful in practice. It also attempts to ensure more effective enforcement by independent authorities with more teeth, as well as better possibilities for redress for individuals, including through the right of associations or organisations representing citizens and consumers to take collective action. We also welcome the emphasis on responsibility and accountability of controllers for building privacy in their systems ("privacy by design"), and the requirement for breach notifications.

However, the Regulation also has a number of weaknesses, which have the potential to undermine severely the rights of individuals. Some aspects require clarification or improvement. In the chart below we identify priority areas where data protection is not robustly mandated in the proposed Regulation, and where we call for improvements that, if implemented, would make the proposed Regulation more comprehensive and more protective of citizen and consumer privacy. Each section gives a summary, followed by suggestions for improvements or amendments for specific articles.

Our key messages reflected in this chart are:

(1) The definition and accompanying recital of 'data subject' (and therefore 'personal data') leaves potential loopholes for people to be singled out but not protected

(2) Legitimate interest can provide a convenient loophole for abusive or excessive processing

[1] *See* COM(2012) 11 Final, 2012/0011 (COD).
[2] *See* COM(2012) 10 Final, 2012/0010 (COD).
[3] See Privacy International, Summary analysis of European Commission proposal for a Data Protection Directive in the law enforcement sector, available at www.privacyinternational.org

(3) Further non-compatible use of personal data completely undermines the purpose limitation principle, one of the fundamental pillars on which data protection is based

(4) Provisions for subject rights against profiling are weak, and leave open the door for discrimination

(5) Restrictions possible for public interest reasons, which are not properly defined, could render all the rights and obligations in the Regulation null and void

Note: *the chart uses for the most part the same terminology as defined in the regulation, e.g. data subject, controller, etc. Data when used on its own means personal data.*

Article of the Proposed Regulation and issue area	**Existing requirement of the Proposed Regulation**	**<u>Improvements needed</u> and comments**
<u>Fundamental Concepts</u> • **The definition, and accompanying recital of personal data and data subject should make clear that any information used to single out an individual, even if he/she is not "identified", is personal data.** The definition must also anticipate fast developing technologies that make reverse engineering of forms of 'anonymisation' more possible; this is essential for the Regulation not to become quickly obsolete. • **We welcome the stronger definition of consent, which should deter getting consent by stealth techniques; it could be made stronger by making it also 'provable'.**		
Art 4(1) and (2). Definition of personal data and data subject.	The definition of data subject (which determines, for the most part, what is considered to be 'personal data') covers any information that is reasonably likely to be used by a data controller to identify, directly or indirectly, a natural person. It names certain specific categories, such as identification number, location data, etc.	(1) <u>This definition must be expanded to make clear that any information used to "single out" an individual person makes this information personal data. The definition should also include IP addresses in the list of specific categories.</u> (2) <u>Recital 24 must be further amended (in particular the last sentence) to clarify that any identifier that has a close relation to a person should be considered personal information; some specific examples can be listed.</u> People can be "individualised" or singled out through a unique number and online behaviour without actually being identified. Profiling, tracking or monitoring don't need a specific name or address and can determine how consumers and citizens are treated. Therefore the

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	**Improvements needed** and comments
		definition and preamble must include data that enables one individual to be distinguished from another. The definition must also anticipate fast developing technologies that make reverse engineering of anonymisation more possible.
***Art 4(8)**. Definition of consent*	The definition of consent (one of the conditions for lawful data processing) clarifies it should be strong, by adding "explicit" to the existing Directive 95/46/EC requirements of "free, informed and specific", and it should be evidenced by a statement or clear affirmative action.	This definition could be further strengthened by adding that it should be "provable" to echo the burden of proof requirement for controllers in Art 7(1). Recital 25, which explains conditions of consent, should specifically state that pre-ticked boxes online do not conform to the consent definition; and that "informed" means giving the data subjects the information listed in Art 14, prior to their consent. It is vital to keep this definition and strengthen it further as indicated, as it has to reflect the evolution in technologies that have become so sophisticated that people don't know or are not aware that their data is being collected, and to what degree, and privacy notices are obscure and few people read or understand them. Furthermore, there is ample evidence that current online consent-collecting methods, such as pre-ticked or opt-out boxes are neither free nor informed.

Rights of the Data Subject

- **Lawful processing on grounds of (vaguely defined) legitimate interest of the controller can provide a convenient loophole for excessive processing; there is need for a clear definition with illustrative examples. Direct marketing should be excluded.**
- **The new provision in Art 6(4) for further non-compatible use undermines the very basis of data protection and leaves the door open to unexpected forms of further use of data; this article should be deleted.**
- **To ensure consistency across the Regulation, information provided to the data subject should also include that on profiling and on security measures. Uniform formats will help data subject learn their core rights through consistency and repetition.**

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
• **The right of access for the data subject should re-instate the right to see their automatically generated profiles.** • **The right to data portability from one service to another is most welcome, but safeguards are needed to protect against potential abuse. For this right to be possible in reality, the data to be transferred needs to be interoperable, so technical standards will need to be mandated.** • **Art 20 covering the right not to be profiled by "automated" means needs further clarification and include the controller's obligation to inform data subjects on techniques and procedures for profiling (so-called algorithms) as well as document results of profiling in case of complaints and redress actions.** • **Data breach notification is welcome, but should ensure that individuals are only notified when there is a serious risk, to avoid notification fatigue**.		
Art 6 (1) (f) *Processing for the purposes of the legitimate interest of the controller*	Art 6 defines six grounds for "lawful" processing of personal data. The "legitimate interests" pursued by a controller is one of them, unless they are overridden by the interests or fundamental rights and freedoms of the data subject, particularly children.	(1) The meaning of "legitimate interests" should be clearly explained in the proposal, with examples of some typical situations that would not be covered by the other five grounds for lawful processing. (2) To align the proposed Regulation provision with the revised e-privacy directive 2009/136/EC that requires consent for direct marketing, specifically exclude direct marketing as a legitimate interest. Legitimate interest can provide a convenient loophole for abusive or excessive processing, and there are examples of this taking place under the current legislation; so there is need for a clear definition with illustrative examples for e.g. in recital 38. The requirement to tell data subjects about such processing in Art 14 (b), as well as the right to object, including to direct marketing, in Art 19 (1) and (2) is very welcome and wise, however prevention is better than (often costly) cure.

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
Art 6 (4) *Further non-compatible use of personal data*	Further use of personal data is permitted even if the purpose of the processing is incompatible with the one for which the data was originally collected, providing it has a legal basis in one of the grounds listed in 6 (1) (a) - (e) (i.e. consent, contract, legal obligation, vital interests of the subject and public interest)	We strongly urge the lawmakers to delete Art 6(4), and not weaken the purpose limitation principle[4]. Guidelines regarding the boundaries of compatible further use of personal data should be developed by the envisaged European Data Protection Board Purpose limitation as expressed in Art 5(b) is one of the pillars of data protection law, and current legislation allows further use only if it is compatible with the original purpose and the citizen (data subject) has been informed. This new provision in the proposed Regulation completely undermines the very basis of data protection and leaves the door open to unexpected forms of further use; for example where a person has provided private data to conclude a service contract and finds that this is being used for the exercise of a 'public interest' task which is also not defined (see also Art 21 below). This is not transparent, not foreseeable and not fair.
Art 11 and 14 *Transparency and information to the data subject*	Controllers have an obligation to ensure transparent policies and clear communications (Art 11), and precision as to which information should be given to the data subject when the data are collected (Art 14)	*(1)* Article 14 should include further specific information in the list provided in para 1; this must include information on measures based on profiling and their consequences, as already required in Art 20(4) on profiling and Art 15(1)(h) on subject access rights[5]. As applicable, information should also be provided on specific security measures taken to protect personal data. (2) Development of standard forms for providing the information listed (14 (8)), should be definite rather than optional ("will" rather than "may") and should be carried out with meaningful input from all the relevant stakeholders, and including behavioural economists and designers. In this context, layered/shortened notices should be specifically

[4] As proposed in p 120-123, EDPS Opinion, and page 11, Article 29 WP Opinion 01/2012
[5] As proposed in p 144, EDPS Opinion

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
		mentioned. As much of citizen's and consumers' personal information, including sensitive information, is held on remote servers (in the 'cloud'), it is important that data subjects are informed of the security measures taken to protect their information. Regarding standard forms, a level of uniformity across controller policies could help teach people their core rights through repetition and consistency.
Art 15 *Right of access for the data subject*	The subject access right allows data subjects to request at any time from the controller the information connected with the processing of their data, including the categories of personal data concerned, to whom their data has been or being disclosed (particularly recipients in third countries), the retention period, etc.; the types of information that must be provided is relatively detailed.	(1) Art 15 (2) should also specify that the data subject has the right to obtain from the controller both personal data that was provided by the individual him/herself, and copies of their profiles collected through other automated means (or at least the categories into which they have been placed) (2) The requirement for clear and plain language, and legible standard formats should also apply to data provided under subject access rights (for e.g. the same requirements for commonly used electronic formats and standards as Art 18) The right to request access to profiling data is consistent with Art 20 (see below). And this provision already exists in the current legislation, so it is not clear why it has been taken out since profiling techniques have developed dramatically. The requirement for intelligible and standard format is consistent with the principle of transparency and Art 11 and Art 18 on data portability.
Art 18 *Right to data portability*	The new right to data portability allows users to transfer their data, which is processed by electronic means, including automated collection, from one service provider to another, in a commonly used format. The Commission may specify this format and the technical standards and procedures for the transmission to ensure interoperability.	(1) To prevent abuse of this right, particularly with regards to children and other vulnerable people, it should be clarified in this article that a controller cannot make data transfer from another controller a condition for providing the new service. Preamble 55 should be expanded with examples accordingly.

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
		(2) It should be clarified that the right to data portability is without prejudice to the rights to erasure and the principle of deleting data when they are no longer necessary (Art 5 (e)). A business could conceivably require a consumer to port their data from an old service provider as a condition of use for the provision of the new service, e.g for profiling/marketing purposes. For right to portability to be *de facto* operational, the data need to be interoperable, not currently the case in many instances, e.g. instant messaging services, social networks, cloud-based storage/services etc. The provision to mandate or specify technical standards to achieve this may need to be expressed in stronger terms.
Art 20 *Profiling*	This article refers to the right of every person not to be subject to measures resulting from profiling, or automated processing. Such processing maybe intended to evaluate, analyse or predict for e.g. the person's performance at work, economic situation, health, or behaviour, and can have legal consequences , or significantly affect the person. Sections 20 (2) and 20 (3) outline certain conditions under which profiling is permitted, such as performance of a contract, express authorisation by other Union or Member State laws, or based on data subject's consent.	(1) The proposed Regulation should give individuals the right to specifically ask controllers whether they are being profiled and, if they are, to have the right to obtain copies of their profiles, or the categories into which their personal data have been placed, for e.g. for advertising purposes. (2) Art 20(1) should clearly state that it applies to both online and offline profiling. For this purpose it is also necessary to recognise that online identifiers are personal data as suggested in section on Art 4(1) above. (3) As also remarked under Art 15 above, section 20(2)(a) must include the right for data subjects to be provided with meaningful information about the logic and techniques used in the profiling as part of controller obligations. If human intervention has taken place, there should be an explicit right to an explanation of the decision reached after such intervention. In this respect, controllers should document the results of profiling.

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
		(4) Amend Art 20 (3) to state that in the private sector automated profiling may never be based on sensitive personal data or include personal sensitive data. In the public sector, profiling shall only involve use of sensitive personal data when this data is manifestly relevant, necessary and proportionate to the purposes of the legitimate public interest pursued. This article needs further clarification, as profiles based on automatic collection, e.g. through cookie placements, can be incorrect, hard or impossible to verify, and result in forms of discrimination against a person. It needs to be clear that "automated" profiling means both online and offline profiling, especially since the current definition and explanatory recital is too vague regarding online identifiers (see Art 4.1 above). The obligation to inform data subjects on the techniques and procedures for profiling already exist in the current Directive, and should be reinstated in the Regulation. And controllers should document the results of profiling, to enable assessment by competent authorities in cases of complaints and redress actions.
Art 21 *Restrictions to rights and principles for public interest reasons*	Union or Member State law may restrict, for "public interest" reasons, the data subject rights and controller obligations regarding all the fundamental principles in Art 5; the rights of the data subject (including erasure, to object and profiling), and the obligations to notify data breaches (Art 32)	This article must further restrict the use of public interest exemptions to specific well defined circumstances, such as criminal offences and important economic and financial interests, and that it must include detailed safeguards and guarantees in relation to the purposes, necessity, proportionality and categories of data to be processed. Furthermore, a provision should be added that controllers should not be forced to retain data or take other measures beyond what is strictly necessary for their original processing purposes, in case it was needed for law enforcement purposes.[6]

[6] As recommended in p 159-165 and page 70, EDPS Opinion; see also page 12, Article 29 Working Party Opinion 01/2012

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
		This article can practically render null and void all the data subject rights, as well as the majority of the fundamental principles of data protection without providing adequate safeguards that should be followed when this article is applied. In addition it contains a catch-all vague phrase of "other public interests" which are not defined elsewhere in the Regulation, and therefore are open to abuse, notwithstanding the mentions of fundamental rights in Recital 59. Therefore we strongly support the EDPS recommendations on its clarification, including that the restrictions should be harmonised at the EU level.
Art 23 (2) *Data protection by default*	The controller must ensure that the principles relating to data processing (Art 5), especially minimisation, are embedded by default in its data processing systems; and in particular that those systems ensure that by default personal data are not made publicly available.	The article should state unambiguously, rather than leave it to delegated acts, that privacy settings on any online or technology-driven services or products should comply by default with the Regulation principles; add to Art 23(2) that data subjects should have control over the extent to which their data is distributed. Default settings for many online services are set for maximum public access, and it should be up to the user to decide how wide he/she wants the data to be distributed.
Art 31 and 32 *Personal Data Breach notification*	Two new provisions that require data controllers to notify data protection authorities of all personal data breaches within 24 hours (Art 31), and to notify data subjects of personal data breaches, when this is likely to affect the protection of his or her personal data or privacy (Art 32)	Individuals should be notified of a personal data breach only when the breach is likely to have a serious or adverse effect. The European Data Protection Board should be delegated to develop criteria and requirements for identifying a data breach and when it should be notified to persons affected. While data breach notifications can be a valuable deterrent against sloppy security by controllers, the above amendment is needed to guard against "notification fatigue" which has been seen in parts of the US where similar laws exist. Nonetheless, data protection authorities must keep a public register of the

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	Improvements needed and comments
		types of breaches that have occurred and the protections in place so as to inform the public debate about the nature of information security across public and private services.
Enforcement and Redress • **To ensure complete independence of supervisory authority, the proposed Regulation must state clearly that they should only be accountable to the parliament of the country concerned** • **We welcome the provision for collective rights to complain or take court action for representative associations and organisations. However the proposed Regulation should go the full way and provide the full right for collective redress.**		
Art 47 and 48 **Independence and general conditions for the supervisory authorities**	Supervisory authories must act with complete independence, free from any influence, avoid any conflict of interest, act with integrity and be provided with adequate resources to be able to exercise their duties (Art 47). Such authorities must be appointed either by national parliaments or government, and their independence should be beyond doubt, as well as have the right skills and experience (Art 48; the article also specifies conditions for dismissal)	To ensure complete independence, Art 47 must state clearly that a supervisory authority shall only be accountable to the parliament of the country concerned, both in terms of budgetary control and performance oversight. Complete independence in carrying out supervisory duties can only be ensured if there is no bias (political or otherwise) present in the body to which a data protection authority is ultimately accountable. And such a body can only be the Parliament, due to its representativeness.
Art 73 to 77 *Rights of redress for the data subjects*	The proposed Regulation introduces several possibilities for data subjects to obtain redress for rights infringements. Organisations or associations defending data subjects' rights and interests have the right to make a complaint before a supervisory authority in any member state or to bring a court action (Art 73 and 76), on behalf of one or more data subjects. Any person who has suffered damage due to unlawful processing has a right to receive compensation for the damage suffered (Art 77)	(1) The proposed Regulation should include a wider provision on collective action, and provide for organisations representing data subjects to have the right to bring judicial actions for compensation. (2) The Regulation should clarify that compensation should be provided for both material loss and non-material damage such as distress or time loss; guidelines for quantification of damages and how they should be calculated in collective actions should be delegated for development to EDPB. (3) Organisations should also be able to lodge complaints prior to any breaches of individual

Article of the Proposed Regulation and issue area	Existing requirement of the Proposed Regulation	**Improvements needed and comments**
		rights, based on detection of a clear failure to design systems as envisaged by Art 23. Individual victims of a data breach are unlikely to go to court, as often the costs would be disproportionate to the costs suffered, so collective judicial action is both cost and time efficient. Non-material damage or distress can be far more significant than material damage in cases e.g. of identity theft. If an organisation or association has clear cause or evidence to believe that a data controller is not implementing appropriate technical measures and procedures to conform to the Regulation, it should be able to lodge a complaint with the regulatory authority and demand audit or investigation. This happens already in some member countries with regards to e.g. competition law.