Access Position on the European Commission proposal for a General Data Protection Regulation

The European Commission proposed, in January 2012, a comprehensive reform of the data protection framework in the EU, which includes a proposal for a General Data Protection Regulation.[1] This proposal would harmonise data protection rules throughout the entire continent, ironing out the rough patchwork of different laws currently in place across member states.

We recognize the need for a consistent approach to data protection, and generally welcome the proposal for a Regulation. But there is much that needs to be improved, starting with the proposal's treatment of the concept of data protection by design and by default. There is also a great need to ensure that the "right to be forgotten," an article that more or less reaffirms existing rights outlined in the 1995 Directive[2], contains broad exceptions so it does not infringe on the right to free expression. Despite needing these improvements, the Data Protection Regulation is a strong step toward ensuring that public bodies and companies protect the fundamental rights[3] of European citizens.

Broadly speaking, the Regulation has great potential to strengthen the rights of citizens (or 'data subjects') in the information society; to ensure greater accountability and transparency on behalf of data controllers (public or private actors); and to strengthen the enforcement powers of authorities to ensure compliance with the law. As an international organisation, we believe it is absolutely imperative that the Regulation maintains the highest standards because the EU has consistently set international norms in this space. Many countries, especially developing nations, have passed their very first data protection frameworks in response to the rapid advancement of the information society, and were strongly influenced by the European Union[4] (e.g., Brazil, Jamaica and the Philippines). As a potential standard setting piece of legislation, not only could the Regulation provide European citizens with the protection and control they need in the information society, but it also could benefit citizens around the world.

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[3] http://www.europarl.europa.eu/charter/default_en.htm
[4] http://blog.security-breaches.com/2011/05/09/new_brazilian_data_protection_bill_adopts_data_breach_notification_regime/ and http://www.lexology.com/library/detail.aspx?g=7c163ebf-bbb0-496f-971b-6a055395c5ac

In the online sphere, where data can be copied, transferred, and collated cheaply and quickly, it is becoming difficult for citizens to keep control of their own information. The Regulation aims to provide citizens with greater control over their personal data, giving them up-to-date and "future proof" protection in the digital age. Adequate data protection, as envisioned through the Regulation, could be seen as a puzzle, where all the pieces, big and small, must fit together to complete the picture. This is why it is important to make sure that all aspects, from the definitions, to the rights of the data subject, to the obligations on controllers, are all sufficiently strong.

Given the sheer breadth of the Regulation, it will not be possible at this time to comment on every aspect of the proposed legislation. As such, we will comment on only the most significant elements that pertain to our work at Access. For more granular analysis on other aspects of the Regulation, please consult protectmydata.eu.[5]

Access seeks to ensure the following throughout the Regulation:

1. Strong foundations upon which the Regulation is built -- getting the definitions and principles right;
2. A thorough strengthening of the rights of the data subject;
3. Greater transparency and accountability on behalf of data controllers;
4. Stronger remedy mechanisms for users.

Article in Regulation	***Comments, Required Improvements and Justification***
Definitions & Principles	
Art 4(1) - Definition of 'data subject'	In order for the Regulation to maintain relevance and applicability in the fast moving online environment, key definitions, such as 'data subject,' must be appropriately broad, particularly in the age of "big data," where data considered to be non-identifying can be combined in ways that could lead to the identification of an individual. The Regulation should apply to data that allow the

[5] The information on this site is produced by EDRi's Brussels team and EDRi's Data Protection Working Group, of which our Brussels-based policy analyst, Raegan MacDonald, is a member.

	"singling out" of an individual, and it should also make clear that online identifiers (such as IP addresses) should, in the majority of cases, be considered personal data.
Art 4(2) - Definition of 'personal data' & Recital 24	The definition of 'personal data' is closely related to that of 'data subject', and requires a similarly broad definition. Art 4(2) should make explicit reference to Recital 24, which provides a detailed definition, giving examples of online identifiers that, if combined with other information, could lead to the identification (or "singling out") of an individual. Following this, Recital 24 should also be broadened to make clear that online identifiers should in the majority of cases be considered personal data.
Art 4(8) - Definition of the 'data subject's consent'	We welcome this definition; in particular the specification that consent is any freely given "specific, informed and explicit" indication of his or her wishes. The need to provide data subjects with the ability to truly consent (through explicit indication) will greatly increase user awareness and control over the processing of their personal data, particularly in the online environment.
Art 6(1)(f) - Lawfulness of processing: "legitimate interests of a controller" & Recital 38	Article 6 lists the grounds on which the processing of personal data is permitted. "Legitimate interest" (Art 6(1)(f)) is an additional instance where the data controller can process personal data (others include: with data subject's consent; when the information is necessary for the performance of a contract; for a legal obligation; for the vital interests of the data subject; and for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller). As it stands, this paragraph is far too broad, and could leave a loophole in the proposal that would allow companies to avoid the restrictions outlined in the Regulation. Furthermore, the vagueness of the paragraph creates legal uncertainty, and would allow for varying interpretations in the different Member States. This would detract from one of the core purposes of the Regulation, namely to harmonise data protection rules in the EU. Considering these reasons and the fact that sections (a) to (e) already give ample reasons for the processing of personal data, "legitimate interest" (f) should be deleted.
Art 7 (1), (2) - Conditions for consent	The proposal addresses the notion of 'consent' in a comprehensive and suitable manner in order to further specify and reinforce these conditions. The burden of proof imposed on the controller by

	Art.7 is a new and positive element, as well as the safeguards introduced in the context of a written declaration which exclude the validity of the consent where there is a significant imbalance between the position of the data subject and the controller (some examples of this situation are given by Recital 34, such as the employment context or when the controller is a public authority).
Rights of the Data Subject	
Art 11 - Transparent information and communication	This further strengthening of data subjects' rights through measures reinforcing the obligations incumbent on controllers for ensuring the effective exercise of such rights is particularly welcomed by Access, especially the obligation to communicate with the data subject using clear and plain language, adapted to the data subject (for instance, in the case of information addressed to a child).
Art 13 - Rights in relation to recipients	As this Article is directly linked with Articles 16 and 17, we suggest expanding it to include an obligation to inform the data subject about the follow up given to their request by recipients for any rectification or erasure that was carried out.
Art 15 - Right of access for the data subject	In the digital era, where the scale of data sharing and collecting has increased dramatically and data are transferred and processed at rapid speeds, data subjects may not know which of their data are processed. In particular 15(c), data subjects' right to know to whom their data are disclosed, especially *all* recipients in third countries, is indispensable. To further strengthen this article, we suggest using language from Article 11 on providing in "clear and plain language" information about the processing of personal data to the data subject. The Article also requires a broader scope to include a reference to measures in respect to the data subject that are based on information processed under Article 20(1) (profiling).
Art 16 - Right to Rectification	This article increases the data subject's right to have full control of her or his personal data and highlights once again the need to ensure an adequate balance between the position of the data subject and the controller.

Art 17 - Right to be forgotten and to erasure	This article, while the principle is welcomed and in fact built upon rights established in the 1995 Directive, is poorly drafted and needs significant rewording if it is to be implementable in the online environment. For these reasons Access asks that article 17 repeat what Recital (54) clearly states regarding the online environment. In particular, it has to be clarified that the 'right to be forgotten' will not infringe on the right to free expression, but rather represents the data subject's right to decide whether or not information he/she made available in the past could be still processed in some circumstances. For this reason we also recommend expanding the scope of Article 80 to cover more broadly freedom of expression (and not only for journalistic, artistic or literary expression as it is currently written). Article 17 might need to be further developed in that respect, and be set up as a means to strengthen the control that individuals have over their personal data. Art 17(2) must be deleted in order to ensure that controllers are responsible only for this right only to data over which they have control. Additionally, making online services liable for the availability of content over which they have no control could lead to measures (filtering, blocking, de-indexing, etc.) that would infringe on the right to free expression and could undermine privacy. (To ensure erasure on behalf of the controller without imposing liability on the controller, please see our recommended changes to Article 13). Finally, as the interpretation of this Article is subject to some misunderstanding as to what it will and will not allow, we suggest renaming it simply to the "Right to erasure".
Art 18 - Right to data portability	Access strongly supports this right, as it is a key element to provide users with greater control over their personal data. However, the scope of Art 18 must be broadened to include not only data collected on the basis of consent, but by other means (listed in Article 6 (a) to (e) on the lawfulness of processing). Art 18(1) and (2) should specify that "commonly used" format includes interoperable and open source formats.

Art 20 - Measures based on profiling	As it stands, this article leaves a loophole that would allow profiling of individuals without their knowledge or consent. We suggest, first, to explicitly foresee the right not to be subject to measures based on profiling both offline and online. In particular, the term “significantly affects” is imprecise and should be clarified so that it also covers the application of, for example, web analysing tools, tracking for assessing user behaviour, the creation of motion profiles by mobile applications, or the creation of personal profiles by social networks. Furthermore, the provision should not be limited to solely automated processing but should also cover partly automated processing methods.
Obligations of Controller and Processor	
Art 23 - Data protection by design and by default	Access strongly supports the addition of this article in the Regulation. However, specification is required to ensure practical application and maximum results for citizens. Art 23 should be further specified to include 1(a) Technical measures, which refer to the physical design of products, such as hardware and software; and 1(b) Organisational measures, which include external and internal policies, current best practices. Similarly, the definition of privacy by default (2) also needs to be more specific and include references to both the technical and organisational aspects. We therefore suggest the same delineation of 23(2)(a) Technical measures, referring to data settings in hardware and software by companies; and 2(b) Organisational measures, referring to privacy protections available to the data subject.
Art 31 - Notification of a personal data breach to the supervisory authority	It is important that data controllers inform the DPA as soon as possible to ensure the highest level of compliance with the obligations set out in the Regulation. Data breach notifications are also an important element for data subjects, as they are empowered to take steps to protect themselves. Controllers, particularly companies, also have clear incentives to downplay the severity of such incidents, due to the very high costs of data breaches (monetarily and for public image and consumer trust). While 24 hours could be perceived as too short a time frame for notification to the supervisory authority, this could be extended to 72 hours in line with the opinion of the EDPS, however this is the maximum extension in our view.

Art 32 - Notification of a personal data breach to the data subject	The introduction of the duty of the notification of a personal data breach to the data subject is generally welcomed by Access. Article 32(5) should include an obligation requiring consultation with the Data Protection Board if the Commission is to adopt any delegated acts. Furthermore, the criteria for establishing a personal data breach and the circumstances under which a breach must be notified to the DPA and the data subjects concerned (for example if there is a risk that would result in a *serious* effect on the protection of their personal data). Finally, Article 32(2) should be expanded to cover points (a) to (e) in Article 31(3).
Art 33 - Data protection impact assessment	Article 33(2)(a) provides a list of processing operations that includes ambiguous phrases, such as "significantly affect the individual" 33(2)(a), or "on a large scale" 33(2)(a), (b), that may obscure the scope of the DPIA. We therefore recommend refining this article to clarify that the exception for carrying out a DPIA as it is made in Article 33(5) only applies if an equivalent assessment has been made in the legislative context.
Remedies, Liability and Sanctions	
Art 73 - Right to lodge a complaint with a supervisory authority	This article is generally welcomed. However, it is lacking the ability for citizens to launch collective action against violators of data protection law. The inclusion of an option to launch collective action is needed, as this type of redress mechanism could empower data subjects and increase the effectiveness of compliance with data protection law. By enabling such collective action, individuals would be more likely to report smaller scale but widespread violations, as they would be much less deterred by administrative burdens, potential costs, and other such risks. Access considers a step forward the (new) right for organisations or associations defending data subjects' rights and interests to lodge a complaint before a supervisory authority or to bring an action to Court (see Articles 73 and 76). However, Access suggests clarifying the nature of the mandate that the organisation must obtain from data subjects.

For more information please visit https://www.accessnow.org/policy/data-protection-reform or contact Access Senior Policy Analyst, Raegan MacDonald at raegan@accessnow.org or +32 486 301 096.