Key aspects of the proposed General Data Protection Regulation explained:

What are they? Why are they important?
What are common misconceptions?
What can be improved?

Table of Contents

As part of the Data Protection Reform Package, the European Parliament is currently discussing the Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)11 final, hereinafter "the proposed Regulation"). This is a very important piece of legislation that will affect almost everyone – natural persons, associations, businesses, most of the public sector – and that is meant to lay down the rules on processing personal data for at least the coming decade.

For this reason, it should come as no surprise that many interest groups are putting forward their views on this proposal. However, it seems that sometimes there are misconceptions in the debate.

This document is meant to provide an overview of key issues regarding the proposed Regulation, explaining why they are important, clarifying points which have sometimes been misunderstood in the debate, and suggesting improvements to the proposed Regulation.

European Digital Rights
Rue Belliard 20, 1040 Brussels
Tel:+32 2 274 25 70
E-Mail: brussels@edri.org, http://www.edri.org

1. Key definitions: data subject and personal data

What is it? Why is it important?

- The definitions of "data subject" and "personal data" are key for determining the scope of the Regulation. "Data subjects" are natural persons who can be directly or indirectly identified by the controller or a third party using reasonably likely means. "Personal data" are data relating to a data subject.
- As these definitions are used to determine the scope of the proposed Regulation, any data that are not personal data are outside the scope of the proposed Regulation.
- Having appropriately wide definitions of "personal data" and "data subject" is therefore key to ensuring comprehensive protection of individuals, especially taking into account that it is becoming increasingly possible to identify a person using less and less data, or to re-connect data that supposedly can no longer be linked to a natural person back to such person (re-identification). To ensure the future-proof character of the proposed Regulation, these definitions should be broad. The alternative is narrow definitions that will be out of date more quickly than the Regulation will enter into force.
- Anonymous data are not expressly defined in the proposal. Such data, i.e. data that cannot be linked to a natural person, are logically out of the scope of the Regulation: the proposal deals with the protection of personal data; data that are not personal are thus outside the scope.

Common misconceptions:

- Just because data are not linked to a name does not mean that they are not personal data. Even removing further items from sets of data does not necessarily render such data anonymous. "Re-identification" attacks have worked on search engine records and others.[1] With technological progress, these attacks will become more and more sophisticated.
- There are claims that a specific definition for anonymous data is needed. It already seems clear that data that cannot be linked to natural persons do not fall under the proposed Regulation. Explicitly defining "anonymous data" runs the risk of creating loopholes due to flaws in a definition, which could then be exploited by controllers to circumvent the rules of the Regulation.
- Sometimes, it is said that the element of identifiability by third parties in the *data subject* definition is too wide. The aim of this wide definition is to also cover situations in which the controller itself is not able to identify persons, but a third party to whom the data might be disclosed might be. To give an example: a controller knows the birth date and the last three postal codes of areas where a person lived, together with the dates when the person moved. This does not on its own allow the controller to identify the person. However, other controllers, such as public authorities, mobile phone operators or big utility companies could be able to cross-reference the data with their own records to find out who this person is.

What could be improved?

- In many cases, it is not necessary for a controller to be able to identify a person to take actions affecting them; "singling out" a person is enough. Think of targeted advertising: the ad network does not need to know who the person that visited a website is, it is enough to know that this person is the same person who earlier visited sites A and B and sometimes clicks on ads for product C. This should be reflected in the definition of data subject by including the aspect of "singling out".
- The definition lists a number of factors how a person can be identified, e.g. with reference to identification numbers. Here, a general reference to "any other unique identifier" could be added for ensuring comprehensive coverage.

1 Overview: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1791742_code487663.pdf?abstractid=1450006&mirid=1
Search engine records: http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0
Video rentals: http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf

2. Legitimate interest and compatible purposes

What is it? Why is it important?

- In the Commission proposal, "legitimate interest pursued by a controller" (Article 6(1)(f)) is one of the six grounds for lawfulness of processing (the five others are: consent, necessity for fulfilment of contract, legal obligation, necessary for vital interests of the data subject, necessity for performance of a task in the public interest / official authority). If processing is to be based on "legitimate interest" of a controller, it shall not override the fundamental rights and interests of the data subject, especially where the data subject is a child.
- The notion of "compatible purposes" (Article 6(4)) comes from the principle of purpose limitation, one of the founding concepts[2] of data protection: personal data are collected for a specific purpose and should not be further processed for incompatible purposes. Compatible purposes are related to the original one. For example, it is generally accepted that limited processing of personal data can be carried out for reasons of IT security, to ensure availability of services. On the other hand, incompatible purposes have no relation to the initial purpose. An example is telecommunications data retention: the initial purpose of collection (billing) and the further processing (storage for law-enforcement use) are completely unrelated. In some cases, such incompatible use might be justified. The Commission proposal allows incompatible use if the new incompatible use has a basis in one of the grounds for lawfulness, except for legitimate interest. Therefore, the data retention example would be covered under processing that is necessary for compliance with a legal obligation to which the controller (here: telecommunications operator) is subject (Article 6(1)(c)).
- Restrictions on incompatible use have been a key part of data protection at least since the 1980 OECD privacy principles.[3] These embodied a stronger spirit than the Commission proposal, by recommending that personal data should only possibly be processed for incompatible purposes with consent of the data subject or where prescribed by law.

Common misconceptions:

- Some claim that any legitimate interests of a third party to whom data are transferred or in whose interest they are processed should constitute a reason for lawfulness of processing as well. This would seriously undermine purpose limitation: normally, people provide their data to a controller expecting that it will be used *only* for the purpose it was provided for.
- There have also been calls to also allow "legitimate interest" as grounds for further processing for incompatible purposes. This would reduce the principle of purpose limitation to an empty shell: for example, telecommunication companies could be able to sell your mobile phone location data to advertisers to have ads follow you around in real life as well.

What could be improved?

- As explained, the notion of "legitimate interest" is notoriously slippery. It makes processing less transparent for data subjects; it opens back doors for controllers to claim "legitimate interest", which data subjects might find difficult to challenge; its interpretation might differ between Member States, undermining the single market. For these reasons, it would be best to delete it completely.
- If not completely deleted, it should be at least defined more clearly. This could be done with recitals giving examples for what could be considered "legitimate interests". Additionally, the right to object to processing based on "legitimate interest" should be strengthened and it should be specified that public sector controllers shall not be able to rely on "legitimate interest" (this was the Commission's intention with the last sentence of Article 6(1)(f), see recital 38).

2 Point 9 of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: http://www.oecd.org/document/18/0,3343,es_2649_34255_1815186_1_1_1_1,00.html

3 See point 10 of the OECD Guidelines referenced in footnote 2.

3. Consent

What is it? Why is it important?

- Consent is defined as a “freely given, specific, informed and explicit” indication of wishes, either by statement or by clear affirmative action. According to the proposal, it shall not be a legal basis for data processing if there is a “significant imbalance” between the controller and the data subject. It is incumbent on the controller to prove that consent has been given.
- It is one of the six grounds for lawfulness of processing. While in some Member States it was traditionally seen as a privileged ground for lawfulness, it is only one among several in the currently applicable Data Protection Directive 95/46/EC.
- Consent is one way for data subjects to control how data about them are processed. For this reason, it is important that consent is clear and explicit. “Implicit consent” would not provide this clarity and would not put data subjects in full control of their data.

Common misconceptions:

- Some argue that “implicit consent” should be possible. This would water down the consent requirement and would be inconsistent with the controller’s obligation to prove consent – how does one prove “implicit consent”?
- Often, it is forgotten that consent is only one out of six grounds for lawfulness of processing. Not all processing needs to be based on consent. For example, if you order something to be delivered to your home, certain payment information and your address need to be processed to perform the contract (Article 6(1)(b)). No consent for processing would be necessary here. However, if that company wants to keep storing this information afterwards, or to track which products on its website you look at to send you tailored ads, it would need to ask for consent. Similarly, if your bank is obliged by law to retain account movements for a certain period, no consent is needed.
- The same misunderstanding is behind calls to change the rules on the consequences of revoking consent. It is argued that often it would not be possible to delete personal data after revoking consent, for example due to legal obligations to retain data. Similarly, some argue that revoking consent implies willingness to terminate a contract in the context of which personal data are processed. However, if there is a legal obligation to retain the data, the storage would still be covered under Article 6(1)(c). The contract scenario seems to be an improper use of consent: necessity for the performance of a contract to which the data subject is party is grounds for lawfulness in Article 6(1)(b). If the data subject wants to stop this processing, he/she would need to terminate the contract. However, the data subject should be able to revoke consent given for processing that is not necessary for the performance of the contract without this impacting on the contract.
- There are fears that not being able to use consent in unequal relationships would unduly restrict controllers' ability to process personal data. Again, it should be noted that consent is not the only ground for lawfulness. In the employment context, a lot of processing would be based on “necessity for performance of a contract”, for example. In fact, the perceived restrictions seem to at least partly stem from a misuse of consent in the first place: instead of thinking about which processing is really necessary for the performance of a contract, controllers tend to have a habit of making data subjects agree to processing that goes beyond what is truly necessary.

What could be improved?

- While the duty to prove consent is already incumbent on the controller, the requirement that consent be “provable” could be added to its definition for additional clarity.
- The definition of “significant imbalance” should be clarified. This could for example be done by adding recitals which provide examples.

4. Data portability

What is it? Why is it important?

– Data portability has two aspects:

(1) if their data are processed in a commonly used electronic format, data subjects can obtain a copy of the data in a format that allows for further use by them (Article 18(1)).

(2) it also means that if data are processed based on consent or contract, users should be able to take the data they have supplied with them when changing service providers (Article 18(2)).

– This right makes it easier for users to change their service providers when they are no longer satisfied with another provider's services. Think of a social network: you might be dissatisfied with your current provider, but by cancelling your account, you would lose all the content you submitted. Data portability fixes this problem. By the same token, it will also stimulate competition by making market entry easier for new companies.

Common misconceptions:

– It is often felt that this right should only apply to information society services such as social networks. Yet, there are many more traditional uses as well: for example being able to export your bank account movements for further analysis by personal finance software or a financial advisor.

– Some argue that it does not add anything to the right of access and should therefore be deleted. While the two rights are related, the right to data portability adds two new elements: (1) data are to be provided in a structured electronic format allowing for further use (consider the banking example above: this would be almost useless if the bank provided the data on paper or in a non-searchable format), and (2) it thereby protects users against lock-in effects.

– There are fears that this right could infringe on controllers' intellectual property rights. This is not the case: the first aspect referred to on the top of this page is only a small widening of the right of access, which so far did not cause such problems. The second aspect only refers to data provided by the data subject, so it is clear that it applies to the raw material, such as bank account movements, but for example not to the bank's internal risk rating of your account.

– Sometimes, there are concerns about controllers' situation when they are legally obliged to store certain data (e.g. banks or telecommunication operators) if users want to take their data to another service. As drafted, this aspect only applies to data processed based on consent or contract. It does not apply to data that are processed based on a legal obligation under Article 6(1)(c). Even if it did, controllers would still be able to rely on Article 17(3)(d) for denying a follow-up request for erasure.

– Finally, some say that this right would put newcomers in the market at an advantage. In our view, this is a feature, not a bug. To quote Competition Commissioner Joaquín Almunia: "Customers should not be locked in to a particular company just because they once trusted them with their content."[4]

What could be improved?

– It should be clarified that the formats in which data are provided should be interoperable. This is to avoid a situation where users would be tied to possibly expensive proprietary viewer programmes for the data they obtained.

– The scope of the second aspect of the right should be extended to cover processing based on all six grounds. As already mentioned, this would not interfere with retention obligations of controllers.

– It should be clarified that controllers should not continue to store data that are no longer needed just for the purpose of being able to comply with a possible future porting request.

4 Speech given on 26/11/2012: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm

5. Right to erasure / Right to be forgotten

What is it? Why is it important?

- This right has two aspects. The first one is the right to erasure in a strict sense (Article 17(1)), which is already included in the current Directive. It basically says that if a controller has no reason to further process data or the data are processed in breach of the Regulation, the data subject is entitled to have the data deleted. There are certain exceptions, e.g. when a controller is legally obliged to retain data or when it is necessary for exercising the freedom of expression.
- This is very important for holding controllers accountable and empowering data subjects to take the protection of their data into their own hands. Supervisory authorities cannot have their eyes on all controllers all the time, so it is crucial to give data subjects strong rights for their interactions with controllers.
- The second aspect is new (Article 17(2)). It states that if controllers have made such personal data public, they shall take all reasonable steps, for publications for which they are responsible, to inform third parties who are processing such data that the data subject requests them to delete any links to or copies of the personal data in question. The Commission's aim with this paragraph was to contribute to meaningful erasure in the online environment.

Common misconceptions:

- While there are legitimate concerns that this right could be abused to stifle free speech, Article 17(1) and Article 17(2) are sometimes conflated in the debate. Article 17(1) deals with situations such as bringing a company to delete your customer data after the business relationship has ended. Article 17(2) is more controversial, dealing with content that has been made public and obliging controllers to take measure to inform third parties who process those data about the request. In both cases, it should be noted that these rights are not absolute; there are exceptions related to freedom of expression (Article 17(3)(a) in connection with Article 80). These exceptions allow Member States to restrict data protection rights in order to reconcile the fundamental rights to data protection and freedom of expression
- There also seem to be misunderstandings about when data subjects are entitled to erasure of their data. Several exceptions are foreseen, including for cases where data are stored based on a legal obligation, public interest reasons in the area of public health, research, and where data have to be maintained for proof (in which case processing shall be restricted instead). So for example, data subjects would not be able to have bank records that must be retained under anti-money-laundering laws deleted.

What could be improved?

- The right to erasure – in a strict sense – should be strengthened by rethinking the exceptions. Currently, there are both restrictions specific to the right to erasure in Article 17 and a general possibility to restrict data subject rights in Article 21. These should be re-evaluated.
- The practical added value of Article 17(2) is not clear, while on the other hand, it brings some risks with it. Given that Article 13 already obliges controllers to inform third parties to whom data have been transferred about rectification and erasure requests, Article 17(2) could be deleted. In turn, Article 13 should be strengthened by including an obligation to obtain information on actions taken by those third parties.
- The possible exceptions for freedom of speech in Article 80 should be strengthened by amending it to simply say that Member States shall adopt such restrictions when they are necessary to reconcile the fundamental rights to data protection and freedom of expression.

6. Data breach notification: when, how and to whom?

What is it? Why is it important?

- "Data breach notification" refers to an obligation of controllers to quickly provide information on data breaches, such as unauthorised access or other data leaks.
- Article 31 obliges controllers to notify all such breaches to the supervisory authority without undue delay and where feasible within 24 hours of discovery of a breach. Late notifications have to be accompanied by a reasoned justification for the delay. The notification includes information on the breach itself, the measures taken to fix it, and possible consequences.
- Article 32 obliges controllers to notify, after the notification to the supervisory authority, breaches that are likely to adversely affect data subjects to them without undue delay. It is important to note that only breaches "likely to affect" data subjects have to be notified to them, and not all breaches.
- Breaches occur. There are no 100% secure systems. Mandatory breach notifications are an effective tool to force organisations to quickly and comprehensively address breaches.

Common misconceptions:

- Some claim that this notification would entail high administrative burden and would distract controllers from fixing the breach, which should be their first priority. However, the elements of the notification (e.g. size of the breach, measures taken to address it) largely concern information that will be generated in any case when trying to stop the breach, so the additional administrative burden is very low. Secondly, notification obligations coupled with a tight deadline put pressure on controllers to actually fix breaches quickly.
- Sometimes, it is claimed that mandatory breach notification would lead to data subjects being covered in an avalanche of breach notifications, resulting in them no longer paying attention to notifications ("breach fatigue"). It should be noted that the Commission proposal already restricts notification to the data subject to cases that are "likely to adversely affect" them, so this risk is already mitigated.
- A similar case has been made about notification to the supervisory authority itself, citing a possible overload. However, restricting notification duties to the supervisory authority to "serious" breaches would put controllers in a position to decide themselves whether a breach is serious or not. The interest of controllers to downplay how serious breaches are is obvious. For this reason, notifications to the supervisory authority should not be restricted. Secondly, Member States are obliged to provide supervisory authorities with adequate resources. When their tasks grow, budgets should follow.
- While the Commission's proposed 24 hour deadline for notification to the DPA is strict, removing the deadline or replacing it with wording such "as soon as possible" would seriously dilute it, as it would enable controllers to delay notification by claiming that it just was not possible any quicker.

What could be improved?

- If restrictions to notification obligations are introduced, they should only concern notification to data subjects. Here, one way to provide information to data subjects where needed while avoiding breach fatigue could be to restrict notification to those breaches likely to "seriously affect" data subjects.
- The 24 hours time limit is indeed very strict. This could be lengthened to up to 72 hours. However, it is important that a fixed deadline remains.
- Supervisory authorities should maintain a public register of breaches. This can help to educate the public about IT security and provide added insight into trends regarding breaches.

7. Data protection by design and by default

What is it? Why is it important?

- Data protection by design means that, already when designing products and services, data protection requirements should be taken into account. This helps to avoid situations in which data protection requirements are an afterthought to the development process, which can result in both higher development costs and lower protection for the data subject.
- Data protection by default means that "out of the box" products and services should be set to the most privacy-friendly settings. Notably this means that by default, personal data are not made accessible to an indefinite number of individuals.
- These two principles can serve to enhance user trust in systems. They also help to protect users who might not be well-aware of data protection issues, such as young elderly users, by ensuring that "out of the box" privacy-friendly default settings are chosen.
- These two principles are also important for the design of standard components: think of a smart meter that in its default configuration sends detailed personal data without encryption, even though it would be capable of encrypting the information. If a utility company, when installing these devices, does not change the setting on its own initiative, the data would be open to being spied upon. Data protection by default would oblige the device producer to switch this functionality on by default.

Common misconceptions:

- It is claimed that these requirements would introduce significant administrative burden for controllers. Yet, they are administrative burden only in the sense that installing catalytic converters in cars is. Instead, it should be seen as an investment: privacy-friendly products can create competitive advantages.
- Contrary to some claims, these principles cannot only be applied to information society services: think of providers of human resources services, smart meters and administrative procedures. All these diverse services and products can benefit from data protection being an integral part of the development process and not just an afterthought.

What could be improved?

- In the Commission proposal, the obligations are formulated in a very vague manner. Combined with the fact that the Parliament and the Council are very sceptic about delegated acts, which are foreseen in the proposal to elaborate on the requirements, it would be advisable to be more specific in Article 23, both for reasons of ensuring a high level of protection and for having legal certainty for controllers.
- At the very least, it should be specified that these obligations should be implemented with both organisational and technical measures.