Definitions (Article 4 - Regulation)

Introduction

Article 4 of the draft Regulation contains 19 definitions. EDRi welcomes the new definitions listed in section 4(9) to section 4(19). At the same time EDRi believes that a number of definitions and corresponding recitals, including the definitions that already existed under Directive 95/46/EC need improvement and/or clarification.

The definition of data subject and personal data

Section 4(1) defines the concept of a data subject. By declaring all data relating to a data subject 'personal data', the concept of what constitutes a data subject becomes paramount. The definition in the draft is very similar to the current definition in section 2(a) of Directive 95/46/EC. In addition to the current definition, the draft clearly states that a person must be considered identifiable when either the data controller or another natural or legal person can identify the person. EDRi welcomes this explanation of what defines personal data. The words 'or another natural or legal person' ensure the absolute concept of identifiability, allowing for protection of personal data whether the data is being processed by the data controller or another person.

In order to ensure data are indeed adequately protected when processed, the phrase 'means likely to be used' must be interpreted broadly in order to provide sufficient protection to data subjects. Both data controllers and third parties can deploy numerous methods identify a data subject. Moreover, the development of such measures cannot be predicted and so a precautionary principle is essential. A broad interpretation of 'likely means' is therefore necessary in order to assure the protection of these data throughout processing. The AOL release of “anonymous” search results should be used as a reference point in policy-making in this area.[1]

What constitutes identifiable?

EDRi advocates a clear understanding of the term 'identifiable'. Data are often presumed non-identifiable, or anonymous while it in fact still traces back to an individual. Personal data should not be regarded anonymous if the data can still be de-anonymized. 'Masking out' or depersonalisation of personal data are valuable security measures, but such measures should not be used to determine whether data are personal data or not. Recitals 23 and 24 should reflect this view point more clearly.

Online identifiers

In relation to the concept of personal data, EDRi is of the opinion that recital 24 regarding online identifiers is too weak to provide for effective data protection in an online environment. This is very likely to lead to confusion with regard to the status of online identifiers. As the AOL case mentioned above proves, online identifiers, even the simple logging of IP addresses without

1 http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all

cookies being used, create (new) personal data. Online behaviour, as a rule, leaves such traces. These traces can be combined with other data relating to the data subject to create user profiles and – often - to identify people or the possibility of identifying them unless the processor knows that the data does not refer to a person. For example, spam filters recognise particular IP addresses as belonging to certain ISP mail servers, which are obviously not data subjects. Such online identifiers must therefore almost in all cases be considered personal data. This should be clearly reflected in both Recital 24 and the definition of personal data.

Identifiability and singling out

Online identifiers can individualise data subjects without identifying them. When data subjects can be singled out without identification, it is possible to treat people differently based on their online behaviour and associated profile. Data that can individualise should therefore also be protected under the Regulation, not least because the ability to individualise carries a strong likelihood of identifiability, as shown by the AOL example.

Definition: consent

EDRi welcomes the strengthening of the definition of consent. Consent is a key aspect of the proposal. However, some additional changes would enable better protection of users in the online environment. Consent should always require active behaviour, both in online and offline environments. The necessity of a “clear affirmative action” could be clearly stated and not only assumed. If changes are needed to the definition of consent, it should be to reaffirm the burden of proof requirement contained in Article 7(1). The definition of consent reflects the efforts to increase the responsibility of data controllers and processors in order to ensure that they see to obtain meaningful consent. To give and/or receive meaningful consent is ultimately what matters. We believe that the criteria of a “freely given specific, informed and explicit” consent allow users to be in a position to give a meaningful consent.

Definition: personal data breach

The definition of the term 'personal data breach' is based on the breach of a security measure. In other words, unwanted loss, disclosure or alteration of personal data without breach of security measures will not constitute a data breach. The same logic applies if there are no security measures in place. Therefore, the reference to the “breach of security measures” should be removed – the cause of the breach is irrelevant.

Definition: main establishment of the controller

The draft regulation provides a definition of main establishment, which is welcomed by EDRi. This definition can prevent confusion about which party must be considered data controller, especially when a group of undertakings process personal data in different locations both within the EU and in third countries. EDRi agrees that the establishment that exercises real control over the data processing must be considered data controller. The location of the main establishment will also determine which data protection authority will act as lead authority (see article 51(2)). However, recital 28 leaves corporate groups of undertakings a lot of room to choose which one of their establishments will be considered the main establishment. A group of undertakings can for example assign the power to implement data protection rules to a certain establishment by power of attorney. In practice this is likely to lead to 'forum shopping' by companies.