The Draft Data Protection Regulation and the Development of Data Processing Applications

Eleni Kosta, Colette Cuijpers

The draft Data Protection Regulation and the development of data processing applications

Eleni Kosta, Colette Cuijpers

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University
PO Box 90153, 5000LE Tilburg, The Netherlands
{e.kosta; cuijpers}@tilburguniversity.edu

Abstract. Nowadays, data processing components are often part of a multitude of products and services. The current review of the European data protection framework, is proposing the replacement of the Data Protection Directive with a Regulation, which will undoubtedly impact the development of such products and services. This chapter analyses some of the critical changes proposed in the Regulation, highlighting the developments with regard to the actual scope of application of the European legal framework, the consent of the users and the particularities of processing pseudonymous data. It also critically assesses the proposed obligations relating to data security, notification of personal data breaches, the principles of data protection by design and by default, as well as data protection impact assessments. The authors conclude that these changes may actually be a step in the direction of more privacy-aware development of products and applications that entail data processing operations, if certain modalities are taken into account before the final adoption of the draft Regulation.

Keywords: consent, data protection impact assessment, General Data Protection Regulation, privacy by design, pseudonymisation.

1 Introduction

In January 2012, the European Commission presented its proposals for the reform of the data protection legal framework of the European Union (EU), proposing the replacement of the Data Protection Directive [1] (hereafter 'DPD') with a Regulation [2], which was the outcome of consultations and debates lasting three intense years.[1] Although the European Commission found that the objectives and the principles of the current legal framework are still valid and sound, it considered that a Regulation will provide more legal certainty compared to a Directive:

[1] The legal framework on data protection proposed by the European Commission, consists on the aforementioned draft Data Protection Regulation, as well as a proposal for a Directive on data protection in relation to police authorities and criminal justice, which repealed the Framework Decision on data protection in the third pillar (Council of the European Union, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60 (30.12.2008)) [3].

> *"a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States."*[2]

Almost two years after the Commission Proposal, on 21 October 2013, the Committee on Civil Liberties, Justice and Home Affairs ('LIBE') of the European Parliament adopted amendments to the Commission's proposal (the 'Parliament text') [4]. A number of Opinions were meanwhile published by various Committees of the European Parliament, such as the Legal Affairs Committee, the Employment and Social Affairs Committee, the Industry, Research and Energy Committee, the Internal Market and Consumer Protection Committee[3], which tabled almost 4,000 amendments. The rapporteur to the LIBE Committee on the draft Regulation published on 16 January 2013 a draft report on the Proposal (known as the 'Albrecht report', after the reporting MEP Jan Philipp Albrecht) [5], which was the basis for the discussion in the LIBE Committee. At the same time, the Council was carrying out parallel work on the draft Regulation and on the 31st of May 2013 the Council released a partial draft compromise text amending the first four chapters of the Commission Proposal ('Council Report') [6]. At the moment of writing, there is heated debate among the European legislative bodies on whether the legislative process for the adoption of the Regulation will be completed before the elections for the European Parliament in Spring 2014, or whether the adoption of the Regulation will be postponed until 2015 [7]. Therefore, this chapter will be mainly based on the text of the Commission Proposal, the Albrecht Report where relevant, and the Parliament text.

Nowadays, a lot of products and services are being developed entailing continuous and complex data processing components. The goal of this chapter is to shed light on whether and how the design and development of such products and services can be influenced by the proposed Data Protection Regulation. Without aiming at being exhaustive, a task that would go way beyond the scope of one book chapter, this chapter wishes to take a closer look at concepts and obligations that will have a direct impact on the development of data processing components and will be important for relevant stakeholders. It discusses in particular changes to traditional data processing concepts and requirements, e.g. consent and data security, as well as critically examines several novel concepts and obligations, e.g. pseudonymous data, privacy by design and by default, privacy impact assessments and data breach notifications. To set the scene of application, first the territorial scope of the Regulation is briefly addressed, explaining when and how the rights and obligations of the Regulation become relevant in the development of data processing applications.

---

[2] Recital 11 Commission Proposal.

[3] A comprehensive list of all the Parliamentary Opinions can be found at http://www.huntonregulationtracker.com/legislativescrutiny/#ScrutinyEUParliament.

2 Territorial scope of application

As multiple international parties may be involved in the development of applications entailing data processing operations, it is critical to clarify the territorial scope of applicability of the European data protection legislation. Article 3 of the draft Regulation differs from Article 4 DPD. A major change introduced by the Regulation is that all EU-established controllers and processors fall within the realm of this Regulation, as no national implementation is required. With the explicit mentioning of 'the establishment of a controller *and processor*', the Regulation as opposed to the DPD, creates a basis for independent obligations pertaining processors. While application to EU-based controllers and cases in which EU-law applies by virtue of public international law are quite similar in the Regulation and the DPD, when it comes to non-EU-based companies engaged in the processing of personal data the Regulation has a significantly different approach [8]. With the Regulation, the criterion 'use of equipment on the territory of a Member State' to determine territorial scope is abandoned.[4] The criteria to determine applicability of the Regulation on data controllers that are based outside the EU are modified and the Commission proposed that the Regulation applies when processing of personal data 'relates to the offering of goods or services to such data subjects or to the monitoring of their behaviour'.[5] This is further clarified in Recitals 19 and 20, which stress that processing of personal data in the context of activities of an establishment in the Union must be in accordance with the Regulation, and also that if actual processing does not take place within the Union, data subjects may not be deprived of the Regulation's protection merely because a controller is not established in the Union.

The meaning of 'monitor the behaviour of data subjects' is clarified in Recital 21: 'If individuals are tracked on the Internet with data processing techniques which consist of applying a "profile" to an individual, particularly in order to take decisions concerning the data subject or for analysing or predicting personal preferences, behaviours and attitudes'. This explanation is not without criticism. Schwartz points to the fact that 'many value-added services that draw on the user's information may be "profiling" and hence "monitoring" in this sense of the Regulation' [9]. According to Schwartz this will lead to the application of the Regulation to many situations where networked intelligence shapes Internet applications and services to accommodate users, without any privacy impact on EU citizens. In this respect Schwarz refers to the system of the DPD, which at least exempted application of the DPD, if equipment was solely used for transit purposes.[6] Therefore, he claims that 'monitoring' should be explained restrictively, including only situations in which an individual's privacy is at risk.

---

[4] Unless such equipment is used only for purposes of transit through the territory of the Community, Art. 4(1)(c) DPD.

[5] Art. 3(2) Commission Proposal. In such case, on the basis of Article 25 of the Commission Proposal, the controller has to designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium-sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects.

[6] Art. 4(1)(c) DPD.

The Council and the Parliament do not support Schwarz's plea [6]. The European Parliament in the Albrecht Report suggests an even broader scope of application relating to 'monitoring data subjects' [10]. According to the Albrecht Report, not only the monitoring of behaviour, but all collection and processing of personal data about Union residents should be covered by the Regulation. In this spirit, the Albrecht Report proposed the amendment of Recital 21 to incorporate reference to data collection other than through Internet tracking. For the rest, the explanation of monitoring remains unchanged: 'particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'. The wording 'particularly' leaves open the possibility of application to situations described by Schwarz, in which privacy is not at stake.

In the Albrecht Report Article 3 is restricted in a sense that application depends on whether monitoring or offering goods or services *is aimed at* data subjects in the Union, while the Commission Proposal used the wording *'are related to'* which covers a broader scope of application. The terminology 'related to the offering of goods or services' is not explained by any of the recitals of the Commission Proposal, while reference could have been made to ruling of the European Court of Justice in the joint cases C-585/08 and C-144/09 (*Pammer and Hotel Alpenhof*):

> *The following matters, not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile: international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.*[11]

The Council Report retains the wording 'when processing activities *are related to* the offering of goods or services'. The Council is however of the opinion that the Regulation should only apply if it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. To ascertain this, the Council explicitly refers to the criteria established by the Court of Justice in the cases *Pammer* and *Hotel Alpenhof*.

Both the Albrecht Report and the Council Report further clarify the concept of 'offering of goods or services' to explain that the Regulation applies to all processing activities irrespective of whether the goods or services require a payment by the data subject [5, 6].

In relation to the territorial scope, the Parliament text expressly states that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes

place in the Union or not. If a controller or processor is not established in the Union, the Regulation applies if the processing activities *are related to* the offering of goods or services, irrespective of whether a payment of the data subject is required; or if the processing activity can be considered to monitor data subjects.

Recital 20 is changed accordingly, stressing that application of the Regulation is irrespective of whether data subjects need to pay for goods or services, and also the phrase 'of the behaviour' is deleted from the original Recital text. Some guidance to determine whether a controller is offering goods or services to data subjects in the Union is provided for in Recital 20 of the Parliament text: "it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects residing in one or more Member States in the Union", although reference is made only to services and not goods. Whether a processing activity can be considered to 'monitor' data subjects is clarified in Recital 21: "it should be ascertained whether individuals are tracked, regardless of the origins of the data, or if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of data processing techniques which consist of applying a 'profile', particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes". As opposed to Recital 21 in the Commission Proposal, after 'profile' the words 'to an individual' are deleted in the version of the Parliament, leaving room to apply the Regulation also in case of group profiling.[7]

Even though the clarifications given in the Parliament text are welcome, the above demonstrates that significant uncertainty remains regarding the territorial scope of the Regulation. In this respect, Kuner regrets that the uncertainty regarding the interpretation of both 'offering goods and services' and ' monitoring behaviour' is not solved by giving delegated power to the European Commission to provide further clarification [8]. However, in view of the discussions regarding desirability of, perhaps too much delegated power with the Commission[8], clarifying the territorial scope within the wording of the Regulation would be preferable. Or, as stated by Aldhouse, "the preferable course would be to leave practical decisions to the data protection authorities who will co-ordinate their efforts through the new European Data Protection Board. Unacceptable decisions should be challenged through judicial mechanisms and determined finally by Court" [14].

3 Consent

The consent requirement is one of the grounds of legitimate data processing and is an essential guarantee of individual control over personal data. The Commission Proposal has sharpened the requirement for consent compared to the DPD by changing

[7] More on data protection and group profiling in [12].

[8] E.g. "The plan to establish the European Commission as the institution to define details through delegated and implementing acts, would put the European Commission into a position of power that does not correspond to the European constitutional requirements. All relevant rules therefore need to be embedded within the regulation itself." [13].

the definition of consent and the conditions under which consent is obtained. The changes to the definition of consent have been taken over in their entirety by the Parliament text. In addition to freely given, specific and informed – requirements already foreseen in the DPD – consent has to be 'explicit'. The DPD requires that consent is 'explicit' only in relation to sensitive data. According to the explanatory memorandum of the Commission Proposal, that the 'explicit' requirement is added to avoid confusion with 'unambiguous' consent and 'in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent'[9].

The Commission Proposal specifies in what ways consent can be given to signify the data subject's agreement to the processing of his/her personal data: 'either by a statement or by a clear affirmative action'[10]. Consent can be expressed via the ticking of a box, in online environments, and via any other statement or conduct that would clearly indicate that the data subject wishes to consent to the processing of his/her personal data in a specific context.[11] With regard to electronic consent the Commission Proposal has taken the position that '[i]f the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'[12]. After the publication of the draft Regulation, the Article 29 Working Party welcomed the modification of the definition of consent, which it saw as intending to "clarify and strengthen data subject's rights" [15], while the European Data Protection Supervisor found that the draft Data Protection Regulation "addresses the notion of 'consent' in a comprehensive and suitable manner in order to further specify and reinforce these conditions" [16]. The Commission Proposal recognises that electronic consent should not be 'unnecessarily disruptive'. Kuner cautions that Recital 25 is in fact softening the consent requirements in online environments, i.e. the Commission Proposal 'would also allow actions such as downloading an application or playing an online game to constitute consent.'[8] Whether the consent rules – if adopted – will be applied in this way remains to be seen. For instance, it will be difficult to claim that consent in these cases is explicit.

The Commission sharpened the consent rule by imposing on the controller the burden of proof that the consent has been provided for specified purposes,[13] as well as that it has been provided in a valid way for a specific data processing operation. To meet the burden of proof, the controllers should obtain the consent by reliable means, taking into account the sensitivity of each specific data processing [16]. Specific methods have to be developed to ensure that consent has been acquired, without at the same time overburdening the users with additional activity.

Under the Commission Proposal, when the consent is provided as part of a written declaration that concerns another matter, the consent requirement has to be presented to the data subject in a way distinguishable in its appearance from the other elements

[9] Commission Proposal, p. 8 (Explanatory Memorandum).
[10] Art. 4(8) Commission Proposal.
[11] Recital 25 Commission Proposal.
[12] Recital 25 Commission Proposal.
[13] Art. 7(1) Commission Proposal.

of the written declaration.[14] The European Parliament further provided that any provisions on consent that are partly in violation with the Regulation will be fully void.

The Commission has followed the Article 29 Working Party position [15] and prohibited the use of consent in cases of a significant power imbalance. This caveat raised a discussion on the kind and range of situations that would potentially involve the imbalance of powers. The Parliament did not keep this provision in its text. Instead it introduced additional qualifications: the consent should be given for specific purposes; and the consent for data processing should not be a precondition for execution of a contract or the provision of a service, when such processing is not necessary for the contract or the service.[16]

The Commission Proposal devoted a dedicated Art. 8 to the processing of personal data of children, paying special attention to issues related to consent.[17] When an information society service is offered directly to a child, the Commission Proposal is differentiating between children above and below 13 years of age. In the latter case, the processing of the children's data is lawful only when and to the extent that the child's parent or custodian ('legal guardian' in the Parliament text) has given or authorised their consent. The Parliament extended the scope of application of Art. 8 to all cases when a child is offered goods or services. Although the Commission Proposal reserves for the Commission the power to adopt standard forms to obtain valid consent[18] and specify the criteria and the conditions of the valid consent of a child[19], there are major technical difficulties of obtaining verifiable consent. The Parliament replaced these Commission powers by the power of the European Data Protection Board to issue guidelines, recommendations and best practices.[20]

4 Pseudonymous data and the concept of profiling

The concept of profiling is not mentioned as such in the DPD, but does occur on several occasions in the Regulation. However, an explicit definition of the concept is not provided for in Article 4 of the Regulation. It appears that Article 15(1) DPD on automated individual decisions is rephrased in the Regulation into the concept of profiling[21,22]. Article 20 grants data subjects the right not to be subject to a measure based on profiling, described as: 'automated processing intended to evaluate certain person-

[14] Art. 7(2) Commission Proposal.

[15] 'The Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.' [17].

[16] Art. 7(4) Parliament text.

[17] Art. 8 Commission Proposal.

[18] Art. 8(4) and recital 130 Commission Proposal.

[19] Art. 8(3) and recital 129 Commission Proposal.

[20] Art. 3 Parliament text.

[21] Art. 15 states: "automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.".

[22] In this respect, the Regulation refers to [18].

al aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour'. The Council Report and the Albrecht Report suggest to include a definition of profiling in Article 4 of the Regulation while retaining rules regarding profiling similar to the proposed Regulation. As explicitly described in the Albrecht Report, a general ban is proposed on profiling, making such activity only permissible when provided for by law.[23] Kuner warns in this respect that the broad definition of profiling includes data processing operations that benefit data subjects and that are merely routine, and that the unclear terminology used is likely to be difficult to implement in practice [8]. One of the proposals in the Albrecht Report might aggravate the situation regarding profiles, as in respect of 'legitimate interest' as processing ground it is suggested to explicitly state that: 'The interests […] of the data subject […] override the legitimate interest of the controller, as a rule, if personal data are processed in the context of profiling'.[24]

While the strict rules on profiles make data processing in a lot of situations difficult, both the Council Report and the Albrecht Report foresee possibilities to ease data processing when use is being made of pseudonyms. This might be a welcome addition to the proposed Regulation that, similar to the DPD, only refers to an exception to process *anonymous data*: 'the principles of data protection do not apply to anonymous information, meaning information which does not relate to an identified or identifiable natural person, or to data rendered anonymous in such a way that the data subject is not or no longer identifiable'.[25] However, researchers like Ohm, but also the Article 29 Working Party, have warned that true anonymisation is increasingly hard to achieve in our current information society where lots of information is disseminated and a variety of technologies exist to link and combine different data sources [19, 20].

In the Albrecht Report the definition of anonymous data is changed to meet this problem, by clarifying that the Regulation also does not apply when identification 'would require a disproportionate amount of time, expense, and effort, taking into account the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed'.[26] However, the assessment whether this actually is the case might be difficult in practice.

Contrary to anonymous data, the concept of *pseudonymous data* is not incorporated in either the DPD, or the Regulation. However, both the Albrecht Report and the Council Report suggest to cover this concept and to regulate the processing of such data. Even though the approach of the Council is more detailed then the approach of the Parliament, e.g. not addressing the legal consequences of processing pseudonyms [10], the rationale to offer leniency when processing pseudonyms is to be found in both reports. The Council Report defines pseudonymous data as: 'personal data processed in such a way that the data cannot be attributed to a specific data subject with-

[23] Albrecht report, 32 and Council report, 40.
[24] Suggested to incorporate in Article 6(1c)(d) of the draft Regulation.
[25] This wording is identical to [6] but corresponds to the meaning of anonymous data in the DPD.
[26] Albrecht report, 15.

out the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution'.[27] Moreover, the Council Report explains that pseudonymous data must be seen as a security measure and privacy by design. In case of a data breach, the Council Report states that the obligation to notify does not apply if only pseudonymous data are affected.[28] To support the idea that pseudonymous data should be considered as a solution to protect personal data while enabling the processing thereof, the proposed Recital 39 states in respect of legitimate controller interests to process personal data, that these: 'could include the processing of personal data for the purposes of anonymising or pseudonymising personal data'.[29]

The position that anonymised, pseudonymised and encrypted data should generally not be covered by the data protection regulation has been heavily criticised in the position published by a number of academics, known as the 'academic manifesto' [13]. These data can still be used to re-identify individuals, and thus are personal data. However, the manifesto does acknowledge that such data might be treated in a different manner, as anonymisation, pseudonymisation and encryption are useful instruments to protect personal data. In this respect the manifesto recommends to have (regularly updated) binding rules that define when data is sufficiently pseudonymised or can be considered anonymous. In a response to the manifesto, Aldhouse presents a risk-based approach [21]. According to Aldhouse, the Regulation should retain its wide scope, but the focus should be on people instead of data, 'so that the strictness of regulation can be matched to the invasiveness and harm of the data processing'.[30]

The explanation provided for in relation to Articles 6 and 20 in the Parliament Report raised a lot of criticism. The balance struck in the Albrecht Report and the Council Report is deemed to be completely undermined by the proposed Recital 58a: 'Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous'.[31] Privacy advocates like the European Digital Rights (EDRI) have warned that the Parliament text will 'amount to a badly drafted license to profile without consent'.[32] In this respect we favor the approach in the Albrecht report in which the rights of data subjects in relation to profiling and the use of pseudonyms seems to be better safeguarded.

---

[27] Council report, 38.

[28] Council report, 70, 77, 80

[29] Council report, 1, 18

[30] This also relates to the previously mentioned opinion of Schwarz in relation to monitoring, which according to Schwarz should only include situations in which an individual's privacy is at risk [9].

[31] Parliament text, 13

[32] See comments by Joe McNamee on www.edri.org, under the heading 'Data protection vote – one step forward, two big steps backwards'.

5 Data security

Both the design and the deployment of technical systems need to be designed in such a way that they will ensure the security of data. The draft Regulation pays special attention to the security of data. It focuses not only on the need for adoption and the implementation of technical and organisational measures for the protection of personal data, something that already existed under the DPD, but also introduces new rules on the notification of the Data Protection Authorities and of the users, when personal data breaches occur.

5.1 Security of processing of personal data

Article 30 of the Commission Proposal is dedicated to the security of processing. Contrary to the DPD that assigned the responsibility for data security to the data controller, the Commission Proposal stipulated that both the controller and the processor are responsible for the security of data that are being processed. The Commission Proposal specifies the steps that need to be taken by the data controllers and processors: First, there needs to be an evaluation of risks, making in this way risk assessments obligatory when personal data are being processed. Based on the outcome of the risk evaluation, then the data controller and the data processor shall take and implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation'.[33] This strongly relates to the introduced concepts of Data Protection Impact Assessments and privacy by design and default, which will be discussed in the next sections of this chapter. The security threats against which security measures need to be taken have not been modified compared to the DPD. So, the measures taken should protect personal data against 'accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data'.[34] The European Parliament enhanced the list of measures that have to be taken, requiring safeguard that only authorised personnel will access the data and that the security policy will be implemented with respect to the processing of personal data.[35]

The Commission has reserved a crucial role in specifying what the aforementioned measures should consist in, by keeping the power to adopt delegated acts on issues such as what constitutes the state of the art, what are the measures that should be adopted in specific sectors or in specific data processing situations.[36] The Commission should establish the aforementioned measures promoting technological neutrality, interoperability and innovation.[37] The European Parliament removed this power of the Commission, providing specific examples on what a security policy should include[38]

[33] Article 30(1) Commission Proposal.
[34] Article 30(2) Commission Proposal.
[35] Article 30(2) Parliament text.
[36] Article 30(3) Commission Proposal.
[37] Recital 66 Commission Proposal.
[38] Article 30(1a) Parliament text.

and entrusting the European Data Protection board with the task of issuing guidelines, recommendations and best practices for the technical and organisational measures.[39]

Moreover, the Commission in its initial proposal was entrusted to adopt implementing acts in various situations and 'in particular to: (a) prevent any unauthorised access to personal data, (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data and (c) ensure the verification of the lawfulness of processing operations'.[40] The European Parliament removed the possibility of the Commission to adopt implementing acts and deleted the relevant paragraph.

The European Commission should involve in this procedure the European Union Network and Information Security Agency (ENISA), which should provide its opinion on the technical and organisational measures for the protection of personal data that should be adopted and on how they should be implemented. This is also in line with the decision of the European regulator to request that the opinion of ENISA should be acquired before the Commission adopted security measures in the area of electronic communications.[41]

5.2 Personal data breach notification

The notification of the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks and services has been regulated in Art 13a of the Framework Directive [22]. The Commission Proposal contains for the first time a general provision on the notification of personal data breaches. A personal data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'[42]. The data controller has to notify both the national supervisory authority and, under conditions, the data subjects concerned that a personal data breach occurred. When the processor becomes aware of a personal data breach, then he has to notify the controller immediately.

The notification to the national supervisory authority has to take place without undue delay, which is specified as within 24 hours from the moment that the data controller becomes aware of the breach. Any delay in notifying the supervisory authority should be justified.[43] The European Parliament removed the time frame of 24 hours, requiring the notification of the national supervisory authority without undue delay. The Commission Proposal specified the information that should be included in the notification[44], while the Commission may adopt delegated acts in order to specify the criteria and the requirements for the establishment of the data breach and for particular circumstances relating to the notification.[45] The European Parliament deleted the

[39] Article 30(3) Parliament text.
[40] Article 30(4) Commission Proposal.
[41] Article 13(a) Directive 2002/21/EC, as modified by Directive 2009/140/EC.
[42] Article 4(9) Commission Proposal.
[43] Article 31(1) Commission Proposal.
[44] Article 31(3) Commission Proposal.
[45] Article 31(5) Commission Proposal.

power of the Commission to adopt delegated acts and entrusted the European Data Protection Board to issue guidelines, recommendations and best practices for establishing the data breach and determining the undue delay. The European Parliament also deleted the possibility of the Commission to adopt implementing acts on the standard format for the notification to the supervisory authority and the form of the documentation.

After notifying the supervisory authority, the data controller has to notify the data subjects 'without undue delay' and 'when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subjects'.[46] The European Parliament extended the obligation to notify the data subject when the data breach is also likely to adversely affect the rights or the legitimate interests of the data subject.[47] Such breaches can result for instance in 'identity theft or fraud, physical harm, significant humiliation or damage reputation'[48]. The concept of undue delay in this case is not specified, neither are the situations that are likely to adversely affect the privacy or the personal data of the data subjects. The Commission is empowered to adopt a delegated act in order to specify the circumstances under which the data subject should be notified of the personal data breach.[49] This power of the Commission was replaced by the Parliament's amendment to entrust the European Data Protection Board with the task of issuing guidelines, recommendation and best practices on when a data breach may adversely affect the data subject. The supervisory authority may even order such notification, taking into account the adverse effects of the breach.[50] The notification to the data subject is not necessary if the data controller demonstrates that he has implemented technological protection measures to the data concerned by the personal data breach that will render the data unintelligible to any unauthorised person.[51] Given the increasing number of data breaches in Europe, the Commission wished to give incentive to the industry to implement encryption measures for the protection of personal data.

6 Data protection by design and by default

Even though one could argue that identification of risks precedes questions of how to mitigate such risks in the design of products and services, the Regulation first presents the principles of privacy by design and default, before addressing Data Protection Impact Assessments (Art. 33). Art. 23 concerns the obligations of the controller arising from the principles of data protection by design and by default. Both at the time of the determination of the means for processing and at the time of the processing itself, a controller must implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of data subjects. Cost and state of the art are mentioned as criteria to be taken into account in assessing the standard of such

[46] Article 32(1) Commission Proposal.
[47] Article 32(1) Parliament text.
[48] Recital 67 Commission Proposal.
[49] Article 32(5) Commission Proposal.
[50] Article 32(4) Commission Proposal.
[51] Article 32(3) Commission Proposal.

measures. Data protection by default is explained in Art. 23 (2) along the lines of data minimisation and purpose specification:

> *Only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.*

The exact meaning of what privacy by default entails is unclear. Recital 61, regarding privacy by design and default, does not add to the wording of Article 23. Some clarification is to be expected from delegated acts and standards provided for by the Commission, specifying further criteria and requirements for appropriate measures and mechanisms to attain privacy by design and default (Art. 23(3) and (4)). Some further clarification on the concept of privacy by design can be drawn from its origin in Canada. While the concept is rather new in Europe, already in the 1990s the Information and Privacy Commissioner for the Canadian province of Ontario, Ann Cavoukian, developed seven Foundational Principles to provide guidance on privacy by design [23]. The principles aim to: 'proactively make privacy the default setting in all areas of technological plans and business practices and explain how privacy should be embedded into the design of systems, in a positive-sum manner — that does not detract from the original purpose of the system' [23]. Cavoukian's second principle is labelled 'Privacy as the Default Setting' and is explained as:

> *Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.*[52]

In contrast to the Commission Proposal, the Albrecht report does provide some explanation to the concept of privacy by default in adding to Recital 61:

> *The principle of data protection by design require [sic.] data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.*[53]

The Albrecht Report also suggests to amend Article 23 to incorporate a reference to Privacy Impact Assessments: 'Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when

[52] http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
[53] Albrecht report, 34.

developing those measures and procedures', referring to the measures to be taken in light of privacy by design and default. The Albrecht Report also claims to further clarify the principle of data protection by default by amending Art. 23 to include: '*Where the data subject is given a choice regarding the processing of personal data*, the controller shall ensure that […] and that data subjects *are able to control the distribution of their personal data*'.[54] However, this does not provide a lot of guidance regarding the contents of the measures to be taken; the standard to adhere to in a default setting; and the framework to assess the appropriateness of measures taken.

In the Parliament text, the most striking amendment concerns the deletion of sections 3 and 4 of Art. 23, deleting the possibility for the Commission to, by way of delegating acts, specify any further criteria and requirements for data protection by design and default, or to determine technical standards for such requirements. The Parliament text tries to provide clarification regarding the requirements by adding criteria to Art. 23:

> *Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor […] shall […] implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation.*

Several points stand out when comparing the initial Art. 23 of the Commission proposal with the amended Art. 23 in the Parliament text. First of all the Commission Proposal only referred to the criteria 'state of the art and cost of implementation'. While several criteria are added in the Parliament text, the criteria 'cost of implementation' is deleted. Furthermore, as opposed to the initially proposed Art. 23, the obligation is not only directed towards controllers, but also to processors. And besides the required appropriateness of the measures, they should according to the Parliament text also be proportionate.

The Parliament text adds a rather extensive part to Art. 23 explaining the scope and focus of data protection by design: 'Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data'. The Parliament text also establishes a clear link between data protection by design and data protection impact assessments (Art. 33) by explicitly stating in Art. 23 that if a data protection impact assessment has been carried out, the results hereof need to be taken into account in developing the measures and procedures required on the basis of data protection by design. By adding a section 1a to Art. 23, the Parliament text also introduces data protection by design as a prerequisite in public tenders according to the Directive on public procurement [24] and the Utilities Directive [25].

The Parliament text also doubles the length of the text of Recital 61 by adding:

---

[54] Council report, 111.

> *The principle of data protection by design require (sic) data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.*

The text regarding privacy by default has not drastically changed in Art. 23 of the Parliament text. It merely clarifies that not only collection and retention of data should be limited to the minimum necessary to achieve the purpose of processing, but that this limitation also extends to dissemination. Moreover it adds a sentence to clarify that data subjects must be able to control the distribution of their personal data.

Within the Council Report, several extra criteria are provided to assess measures to comply with privacy by design and default. Not only the technology and cost of implementation, but also the 'risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing' should be taken into account to determine technical and organisational measures 'appropriate to the processing activity being carried on and its objectives, including the use of pseudonymous data'.[55] In respect to the default, the Council Report complements the proposed Regulation by making a reference to the purpose of processing:

> *if the purpose is not intended to provide the public with information, it must be ensured that by default personal data are not made accessible without human intervention to an indefinite number of individuals.*[56]

There is a rather convincing incentive for data controllers within the Regulation to comply with the principle of privacy by design and default. Article 79 of the Commission Proposal regarding administrative sanctions states: 'The supervisory authority shall impose a fine up to 1,000,000 EUR or, in case of an enterprise up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently […] (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30'.[57] As the first section of Art. 79 of the Commission Proposal states 'each supervisory authority' Kuner warns that in theory a company could be sanctioned separately by 27 different data protection authorities for the same violation if it occurred within each jurisdiction, which stands in contradiction to the fact that supervision of a company is limited to

[55] Council report, 70.

[56] Council report, 70.

[57] The Parliament text contains even stricter rules for administrative sanctions, holding on to only the highest fine category, in which 2% of the annual worldwide turnover is amended to 5%. In the Commission Proposal sections 4 and 5 of Art. 79 contained lower fine provisions, 250.000 euro and 0,5% of annual world wide turnover and 500.000 euro and 1 % of annual world wide turnover. These sections are deleted in the Parliament text.

the DPA of the company's main establishment[58] [8]. According to Art. 37 of the Commission Proposal it is the task of the Data Protection Officer to 'monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation'[59].

7 Data protection impact assessment

Privacy Impact Assessments have been carried out in relation to systems and applications that present privacy aspects and interest, but the concept of a Privacy Impact Assessment (PIA) has become broadly known via the discussions regarding the use of Radio-Frequency Identification (RFID) technology. As this technology makes it possible to track and possibly even identify users, the use of RFID poses a number of concerns regarding their privacy. However, given its economic potential, the use of RFID is steadily becoming an integral part of everyday life. Following a long period of consultation and debate, the Article 29 Working Party endorsed the revised PIA framework for RFID applications and called for its implementation [26]. The PIA framework was officially signed on 6 April 2011 [27].

The Commission Proposal formalises in Art. 33 the requirement for the data controller or the data processor to carry out a Data Protection Impact Assessment in cases when the 'processing operations present specific risks to the rights and freedoms of data subjects', for instance when data subjects are actually excluded from their right or by the use of specific new technologies (Rec. 74). The carrying out of a thorough Data Protection Impact Assessment is expected to limit the likelihood of data breaches (Rec. 71a Parliament text). The Commission Proposal provided some examples of processing operations that present specific risks, such as when sensitive data are being processed, when automated processing leads to profiling of the data subjects, when large-scale video surveillance takes place, or when processing of personal data is carried out in large scale filing systems on children, genetic data or biometric data (Art. 33.2). Recital 71 clarified that Data Protection Impact Assessments should in particular apply to "newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects", which aimed at excluding most small and medium-sized enterprises [8]. The European Parliament deleted the section on risks in relation to Data Protection Impact Assessments and created a new Art. 32a, which is dedicated to the respect to risk and is more elaborate compared to the Commission's references to risk.

The Commission Proposal specifies the minimum information that the Data Protection Impact Assessment shall contain, i.e. a description of the data processing operations, an assessment of risks to the rights and freedoms of data subjects, a description of the measures taken to ensure the mitigation of the risks and the measures taken to

[58] Art. 51(2) Commission Proposal.
[59] Art. 37(3) (c) Commission Proposal.

ensure the protection of the data and to demonstrate compliance (Art. 33.3). The content of the assessment was modified by the European Parliament, which requires also an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an indication for the time limits for erasure and assessment of the context of data processing etc.[60] The provision of the Commission Proposal that the obligation for a Data Protection Impact Assessment does not extend to data controllers that are public authorities that have an obligation to carry out the data processing operation (Art. 33.5 Commission Proposal) was deleted by the European Parliament. The understanding of Data Protection Impact Assessments in the Regulation is that data controllers have to comply with specific points relating to the processing of personal data. In this sense, the Data Protection Impact Assessment as described in the Regulation is narrower in scope, compared to Privacy Impact Assessments [28].

8 Reflections on the data protection reform

Developers of products and services that entail data processing operations offered to European customers, even if the developing entities are established outside the EU, will need to consider the European Data Protection Regulation, if adopted in its current form. The territorial scope of the draft Regulation is meant to extend far beyond the European territory, imposing obligations on data controllers *and* data processors. Besides considering the Regulation from a perspective of possible end-use of products and services, the Regulation might also directly apply to the developers of products and services, even during their test and pilot phases because of the broad interpretation of the notions 'monitoring behaviour' and the 'offering of goods or services', for which no payment by the data subject is required.

Consent has been used often as legitimate ground for data processing especially in online services. The draft Regulation aims at strengthening the rights of the data subjects and ensuring that data subject 'explicitly' consent to the processing of their personal data and imposes the burden to proof that consent has been obtained on the data controller. From this perspective, in the *development* of products and services consent might not be that relevant. However, mechanisms and procedures for end-users of the products being developed to properly provide, register and withdraw consent need to be part of the design of such products. Kuner fears a watering down of the consent requirement because providing consent should not be 'unnecessarily disruptive to the use of the product'. However, based on the rationale and wording of the Regulation as a whole, we expect a rather strict and narrow interpretation of all four consent requirements: freely given, informed, specific and explicit – because of the risks involved – especially in electronic environments.

The specification of the steps that need to be taken by data controllers and processors in view of the requirement of data security closely relate to the introduction of the concepts of Data Protection Impact Assessment and privacy by design and by default. First, there needs to be an evaluation of risks, and based on the outcome of the risk evaluation, data controllers and processors must implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the

[60] Art. 33(3) Parliament text.

risks'. As a final step in the security cycle, when a data breach occurred despite the precautions taken, the Regulation introduces a general obligation of notification of personal data breaches. Again, even though data breach notification might not be a primary concern of developers of data processing appliances, the design might benefit from the exception that notification to the data subject is not necessary if proper encryption measures are taken, which thus might be an interesting functionality to incorporate into a product or service with data processing components.

The introduction in the Parliament text of a general ban on profiling, making such activity only permissible when provided for by law, is likely to be an important consideration in the development of data processing appliances. The leeway given when using pseudonyms might spur the development and implementation of pseudonymisation mechanisms and technologies. Even though the Parliament text proposes that the Regulation applies to pseudonyms, it is deemed an important security measure. The trend to keep pseudonymous, anonymous and encrypted data within the scope of the Regulation, but offering these data different treatments, is definitely a trend worthwhile to consider when developing data processing appliances. It is crucial to keep a close eye on the developments regarding the proposed rules on profiling and pseudonyms, as the Parliament text seems to undermine data subjects' rights by offering too much leeway in respect of the use of pseudonyms in profiling. In our opinion, the wording of the Albrecht Report and the Council Report provide a better balance and better safeguards regarding data subjects' rights in relation to profiling and the use of pseudonyms.

The principles of data protection by design and by default lay down a more general obligation to align the development of products and services with the requirements stemming from the Regulation. As explained in the Parliament text, data protection by design shall have particular regard to the entire lifecycle management of personal data, from collection to deletion, where the obligations are not only directed towards controllers, but also to processors. In order to achieve privacy by design and default, these requirements need to be taken into account in the earliest stages of design. The explicit link between data protection by design and data protection impact assessments requires an active investigation of risks, to be followed by factual (technical and organisational) implementation of measures to counteract the identified risks. Because the standard is set at the default level, collection, retention and dissemination of data should be limited to the minimum necessary to achieve the purpose of processing personal data. Combined with the possibility of high administrative sanctions in case of non-compliance with the principles of privacy by design and default, these principles will definitely impact the development of data processing appliances.

When processing operations present specific risks to the rights and freedoms of data subjects, the draft Regulation requires the carrying out of a Data Protection Impact Assessment. Appliances connected to the Internet – providing feedback and feedforward information based on specific and generalised data subject behaviour – most certainly presents specific risks, e.g. relating to the processing of sensitive data and profiling. As with the Parliament text, no exceptions remain regarding small and medium-sized enterprises, Data Protection Impact Assessments will become an important obligation for all developers of data processing appliances, even those not affiliated to large companies. Not only the assessment as such is relevant, but also the documentation regarding Data Protection Impact Assessment and the actual imple-

mentation of risk mitigating measures. This follows from the higher standards of accountability to be found in the Regulation, which relate to scope – obligations also pertaining data processors – as well as content – e.g. more strict documentation obligations.[61]

Overall, based on the topics discussed in this chapter, the Regulation sets a hopeful tone regarding increased awareness and incentives to better incorporate privacy and data protection into the design of data processing applications, although there still is room for improvement in specific areas. Whether this will be the case probably depends on the strictness of audit, control and enforcement of the Regulation.

9 References

1. European Parliament and Council of the European Union: Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (23.11.1995)
2. European 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 (General Data Protection Regulation) COM(2012) 11 final – 2012/0011 (COD) (25.01.2012)
3. European Commission, Proposal for a Directive of the European Parliament and of the Council 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, COM(2012) 10 final – 2012/0010 (COD) (25.01.2012)
4. European Parliament: Report on the 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 (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), A7-0402/2013 (21.11.2013)
5. Albrecht, Jan Philipp – European Parliament, Committee on Civil Liberties, Justice and Home Affairs: Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD) (16.01.2013)
6. Council of the European Union, 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 (General Data

[61] E.g. the explicit reference to the principle of accountability in Art. 22 requiring technical and organizational measures to ensure and *demonstrate* – in a transparent manner – that the data processing is consistent with the Regulation, but also e.g. the obligation to appoint a Data Protection Officer when personal data are processed in relation to more than 5,000 data subjects, Art. 35 Parliament text.

Protection Regulation) - Key issues of Chapters I-IV, 2012/0011(COD) (31.05.2013)
7. European Council, Cover note 24/25 October 2013 Conclusions, EUCO 169/13 (25.10.2013)
8. Kuner, Christopher: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. PVLR 11, 6 (2012)
9. Schwarz, P.M.: EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation. PVLR12, 718 (2013)
10. Burton, Cédric, Pateraki Anna: Status of the Proposed EU Data Protection Regulation: Where Do We Stand? PVLR 12, 1470 (2013)
11. Joined Cases C-585/08 and C-144/09, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v. Oliver Heller* [2010] ECR I-12527
12. Schreurs, Wim, Hildebrandt, Mireille, Kindt Els, Vanfleteren, Michael: Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Prolfing in the Private Sector. In Hildebrandt M. and Gutwirth S. (eds.) Profiling the European Citizen. Cross-Disciplinary Perspectives 241-269 Springer, Heidelberg (2008)
13. 'Data Protection in Europe – Academics are taking a position' (2013) 29 CLSR, 180-184.
14. Aldhouse, Francis: Data protection in Europe – Some thoughts on reading the academic manifesto. CLSR 29, 289-292 (2013)
15. Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals, WP 191, 23 March 2012
16. European Data Protection Supervisor: Opinion on the data protection reform package (2012)
17. Article 29 Data Protection Working Party: Opinion 8/2001 on the processing of personal data in the employment context, WP 48, 13 September 2001
18. Council of Europe: Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies)
19. Ohm, Paul: Broken Promises Of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review 57, 1701-1777 (2010)
20. Article 29 Data Protection Working Party: Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011
21. Council of the European Union – Press Office: Background – Justice and Home Affairs Council, Brussels 7 and 8 March 2013 (06.03.2013), http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/135854.pdf (as references in [14]
22. European Parliament and the Council of the European Union, Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") [2002] OJ L108/33 (24.04.2002), as modified by European Parliament and the Council of the European Union, Directive 2009/140/EC amending Directives 2002/21/EC on a

common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services ("Better Regulation Directive") [2009] OJ L337/37 (18.12.2009)
23. Cavoukian, Ann: Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers. http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf (2011)
24. European Parliament and Council of the European Union: Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, OJ L 134/001 (30.4.2004)
25. European Parliament and Council of the European Union: Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, OJ L 134/114 (30.4.2004)
26. Article 29 Data Protection Working Party: Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11 February 2011
27. Privacy and Data Protection Impact Assessment Framework for RFID Applications, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf (12.01.2011)
28. Wright, David, de Hert Paul (eds.): Privacy Impact Assessment. Springer, Heidelberg (2012)