Will the European Commission be able to standardise legal technology design without a legal method?

Matthias Pocs, LL. M.,
Universität Kassel, Germany
Computer Law & Security Review 2012, 641-650.

ABSTRACT

Privacy by Design (PbD) is a kind of precautionary legal technology design. It takes opportunities for fundamental rights without creating risks for them. Now the EU Commission "promised" to implement PbD with Art. 23(4) of its proposal of a General Data Protection Regulation. It suggests setting up a committee that can define technical standards for PbD. However the Commission did not keep its promise. Should it be left to the IT security experts who sit in the committee but do not have the legal expertise, to decide on our privacy or, by using overly detailed specifications, to prevent businesses from marketing innovative products? This paper asserts that the Commission's implementation of PbD is not acceptable as it stands and makes positive contributions for the work of a future PbD committee so that the Commission can keep its promise to introduce precautionary legal technology design.

Keywords: privacy impact assessment; PIA; prior checking; automated individual decision; technical standardisation; technology design; legal compatibility; fundamental rights.

1. Introduction

If one implements the principle of Privacy by Design (PbD) correctly it promotes protection of fundamental rights by means of technology design. It is also sensible to implement this legal technology design on the level of the EU. However this will only succeed if one bridges the gap between law and technology. Such a bridge is needed in order to check whether a PbD standard really promotes the law. In addition the PbD standards have to address technology designers because they are the only ones who can implement them.

Art. 23(4) of the regulation proposal[1] does not correctly implement the principle of PbD because it lacks a method of legal technology design. If one searches the regulation proposal for such a method, one finds the legal notion of Privacy Impact Assessment (as "Data Protection Impact Assessment" in Art. 33) which comes closest to such a legal method. PIA allows for consideration of data protection prior to deploying risky technology. Its main advantage is that it specifies prior checking according to Art. 20 of the DPD by requiring a procedure for the acceptance of technology applications. However PIA does not actually require a method of legal technology design. Another reason why the EU Commission's proposal did not implement PbD correctly relates to the addressee of PbD. It obliges technology users ("controller") who can at best choose and adjust the technology, but not technology producers who can really design the technology.

This paper makes no comment on whether or not the proposed regulation is sensible in total but only makes comments on the correct implementation of the principle of PbD. The draft-DPR and its Art. 23 only serve as examples for a future regulation. In the future PbD could also be implemented in a directive or alone in a separate legal instrument. Concerning the implementation of the principle of PbD this paper falls back on the experience that the German Project Group Constitutionally Compatible Technology Design (*"Projektgruppe verfassungsverträgliche Technikgestaltung"* (*provet*)) gained with the method of "concretising legal requirements" (*"Konkretisierung rechtlicher Anforderungen"* (*KORA*)).

[1] *EU Commission*, COM(2012) 11 final, 25.1.2012; unless otherwise specified, Articles refer to articles of the draft-DPR; on the draft-DPR *Hornung* (2012) Zeitschrift für Datenschutz 99.

2. Protection of fundamental rights by technology design

The proposal of a Privacy-by-Design provision is rooted in the idea of promoting fundamental rights protection by technology design. As opposed to choosing and adjusting technology, this legal technology design refers to decisions about the specifications of a technical system. From the individuals' point of view, this has two advantages. On the one hand it can avoid the very creation of predictable risks for fundamental rights. On the other it can take or even amplify the opportunities that technology applications offer. This in turn promotes the precautionary principle[2] of EU law.[3]

The approach of legal technology design offers several advantages. It helps the state to bear its "structural responsibility" (*"Strukturverantwortung"*[4]) and gives individuals technological aids for "self-protection" (*"Selbstschutz"*[5]). It helps legislators to fulfil their duty to observe technological development[6] and to prepare the political process by showing equally effective but less intrusive alternatives. The legal technology design makes the protective precautions against function creep required by the *Bundesverfassungsgericht* (Federal Constitutional Court of Germany)[7] possible. The reference to technology is also necessary to comply with statutory provisions[8] on "data avoidance." Legal technology design makes it possible to automate partly the legal supervision which would otherwise not be effective.[9] In Germany legal technology design is claimed with *"Systemschutz"*[10] ("system protection"), *"Sozialorientierung beim Systementwurf"*[11] ("social orientation during system design") and *"Verfassungsverträgliche Technikgestaltung"*[12] ("constitutionally compatible technology design") as well as in the EU with "Privacy by Design."[13]

Consistently the PbD provision that the Commission suggests in Art. 23(4) promises to comply with these claims. The following section will describe the reason why legal technology design on the EU level is sensible. It will also outline the need for a method and the need for PbD to address technology producers.

First one should not standardise technology design on the regional level but on the EU level. The EU-wide technology design answers the globalisation of data flow because technology is effective worldwide. One critical factor for technology design is the technical standardisation. Thus one should bring legally promoting technological design into the international standardisation.[14]

The most influential players - the US[15] and APEC countries[16] - and also the organisations of OECD and UN do not opt for such a precautionary technology design. Only the EU can control the international standardisation to the benefit of the legal technology design. Therefore, the adoption of PbD standards on EU level could indeed make legal technology design a success. One would increase the pressure on the international standardisation because not only a regional legal system but also the law of the entire EU requires the PbD standard in question and could hence outweigh the US influence on the international standardisation. Insofar the Commission proposal is an opportunity to improve data protection. Therefore the legal technology design on the EU level is sensible and does not violate the subsidiarity principle.

Moreover, legal technology design must not be subject to a free balancing against general technical and economic aspects. The mere reference to technical standards cannot sufficiently limit the control of the economy. This can lead to a non-regulation of the law and can violate the democratic legitimisation of the legislator.[17] In order to achieve real control of the law a method is necessary that does not follow the rules of the (applied) computer science(s) but the rules of legal science.

Technology design requires solving social conflicts. Solving these conflicts, that is transforming the law into reality, is in the field of technology, like in any other area of life,

---

[2] Roßnagel in Eifert/Hoffmann-Riem (eds), *'Innovation, Recht und öffentliche Kommunikation'* (Duncker und Humblot 2011) 44; Costa, (2012) 28 Computer Law and Security Review 14.

[3] Art. 191 TFEU and EuGH *Artegodan GmbH et al. v EU Commission* T-74/00 et al (2002) ECR II-04945.

[4] Roßnagel in Roßnagel (ed), *'Allianz von Medienrecht und Informationstechnik?'* (Nomos 2001) 24.

[5] Hoffmann-Riem (1998) Archiv des öffentlichen Rechts 534; Roßnagel (1997) Zeitschrift für Rechtspolitik 26; Borking (1996) Datenschutz und Datensicherheit 654.

[6] BVerfGE (collection of decisions of the *Bundesverfassungsgericht* (Federal Constitutional Court of Germany)) 112, 304 (316f); BVerfGE 90, 145 (191); Roßnagel, *'Rechtswissenschaftliche Technikfolgenforschung'* (Nomos 1993) 99f.

[7] BVerfGE 125, 260 (327); BVerfGE 65, 1 (46); to a lesser extent (concerning data security) this is also required by ECtHR *I v Finland* 2008 ECHR 20511/03.

[8] For example § 3a of the German Data Protection Act and § 13(6) of the German Telemedia Act.

[9] Bäumler (2004) Datenschutz und Datensicherheit 80 (81); Press release of the *Unabhängiges Landeszentrum für den Datenschutz* (Bizer) 28.2.2006 on Credit History; Podlech in Steinmüller (ed), *'Informationsrecht und Informationspolitik'* (Oldenbourg Verlag 1976) 213.

[10] Podlech in Brückner/Dalichau (eds), *'Beiträge zum Sozialrecht'* (Verlag R.S. Schulz Percha 1982) 452ff; also Dix in Roßnagel (ed), *'Handbuch Datenschutzrecht'* (CH Beck 2003); Roßnagel/Pfitzmann/Garstka, *'Modernisierungsgutachten zum BDSG'* (German Ministry of Interior 2001) 39ff.

[11] Steinmüller, *'Informationstechnologie und Gesellschaft'* (Wissenschaftliche Buchgesellschaft Darmstadt 1993) 570.

[12] Roßnagel/Wedde/Hammer/Pordesch, *'Digitalisierung der Grundrechte'* (Westdeutscher Verlag 1990).

[13] Article 29 Working Party (WP29), *'Future of Privacy'* (WP168) paras 44ff; LRDP Kantor Ltd et al., *'Comparative study about data protection law'* 20.1.2010 paras 131f; on international level: 32nd International Privacy Commissioners' Conference, *'Resolution on Privacy by Design'* 27.-29.10.2009; IPC Ontario (Cavoukian), *'Privacy by Design - The 7 Foundational Principles'* 2011 Ontario; also the OECD claims to respect social values OECD, *'Guidelines for the Security of Information Systems and Networks'* 1037th Council Meeting 25.7.2002 nos 5ff.

[14] Roßnagel in Roßnagel (ed), *'Allianz von Medienrecht und Informationstechnik?'*, (Nomos 2001) 24.

[15] Mankowski, (1999) Arbeitsrecht für die Praxis 140.

[16] Bygrave, *'Privacy Protection in a Global Context'* (2004) 47 Scandinavian Studies in Law, 319 (348).

[17] Denninger, *,Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht* (Nomos 1990) 117ff; Lennartz (1989) Datenschutz und Datensicherheit 231 (232); Blanke (1986) Kritische Justiz 405 (415).

the function of the law.[18]

Therefore, one must not fall back on a method of IT security but on a method that connects legal evaluations with technological possibilities.

The method of legal technology design ensures cooperation with engineers. The law has to get involved in the inherent order of the technical system to be regulated.[19] It has to be concretised to the extent that one can formulate it in the language of computer science[20] and in particular include it in a technical requirements'[21] analysis.[22] Engineers alone cannot promote the protection of fundamental rights; neither can lawyers alone. Both disciplines depend on each other. Legal technology design needs a "bridging-approach" that ensures an intense interdisciplinary cooperation of legal science with computer science and the disciplines of applied computer science.[23]

Furthermore the method of legal technology design ensures that one does not place too many limits on the technology designers' business rights and freedoms according to Art. 15ff. of the EU Fundamental Rights Charter.[24] What is technologically necessary does not have to be legally necessary. During conventional technical standardisation one provides for a large number of requirements for a technical system. Overly detailed specifications place too many limits on the technology producers' rights and freedoms because they are not necessary to promote the rights and freedoms of data subjects. Besides they can constitute barriers to trade and discourage innovation.[25]

Finally legal technology design and PbD standards necessitate a high degree of designability. Accordingly one has to distinguish between the level of technical standardisation and the level of technology application in businesses and public authorities. Whereas technology users can at best choose and adjust technology it is with the technology producers where the actual technology design takes place. Users and data subjects are limited to the possibilities of adjustment that technology producers created for the product chosen. However technology producers are only limited to technical standards.[26] Therefore in order to be able to create acceptance, one has to produce suitable adjustability by standardising the various options of technology design (acceptability). Only technology producers can do.

In consequence the law must also address the technology producers to promote the protection of fundamental rights by technology design. This does not mean that one has to persuade them by using a legal obligation. One can create incentives by rewarding them with seals of quality after successful certification.[27] One can also place on the producers the obligation to design technology in a legally compatible way[28] and to take part in the work of technical standardisation[29] accordingly. Already the technology producers are addressees of the law in the general EU technology law[30] and in particular in the product liability law.[31]

In sum it is sensible to regulate legal technology design on the EU level because then European data protection policy can prevail in the international standardisation. Concerning the proposed PbD provision in particular one has to meet two conditions in order to promote protection of fundamental rights by technology design. First, legal technology design needs a "bridging-approach" that ensures an intense interdisciplinary cooperation of legal science with computer science and the disciplines of applied computer science. Second, legal technology design and PbD standards must mainly address technology producers (as an obligation or incentive) because they are the only ones who can implement these elements.

3. Technology design in future EU data protection law

In the future EU data protection law Privacy by Design will become the central approach to realise legal technology design. The EU Commission tried to implement the principle of PbD in Art. 23. The following section explains why it did not correctly implement the principle of PbD and should address technology producers and set a method of legal technology design.

3.1. Not addressing technology producers

The following subsection will show that the PbD standards planned in Art. 23(4) do not address technology producers but only technology users ("controller"). To this end it will present the proposed provision on PbD and will describe the legal concepts of Accountability and PIA that support the enforcement of PbD.

The provision on PbD consists of four paragraphs of which the fourth paragraph provides for PbD standards. Art. 23(1) re-

[18] Roßnagel, *'Rechtswissenschaftliche Technikfolgenforschung'* (Nomos 1993) 254 and 268f.
[19] Steinmüller in Fülgraff/Falter (eds), *'Wissenschaft in der Verantwortung'* (Campus 1990) 170.
[20] Roßnagel, *'Rechtswissenschaftliche Technikfolgenforschung'* (Nomos 1993) 254.
[21] As defined in DIN 69901-5 and IEEE 830-1998 (C-Requirement).
[22] Pordesch, *'Die elektronische Form und das Präsentationsproblem'* (Nomos 2003) 267f.
[23] Roßnagel in Kortzfleisch/Bohl (eds), *'Wissen, Vernetzung, Virtualisierung'* (EUL Verlag 2008) 387.
[24] For example the provision of a filter system for copyright protection places too many limits on the service provider's freedom pursuant to Art. 16 FRC because s/he would have to install a complicated, costly and permanent computer system on his own expense ECJ C-70/10 Scarlet Extended para 48; affirmative *EuGH*, C-360/10 - SABAM v Netlog.
[25] EU Commission COM(2004) 38 final, 28.1.2004, 31f.
[26] Roßnagel, *'Rechtswissenschaftliche Technikfolgenforschung'* (Nomos 1993) 267.
[27] Roßnagel/Pfitzmann/Garstka, *'Modernisierungsgutachten zum BDSG'* (German Ministry of Interior 2001) 145f.; public users have to prefer certified products according to several German state data protection laws (Brandenburg, Schleswig-Holstein (also "quality seal ordinance"), Mecklenburg-West Pomerania, and North Rhine-Westphalia).
[28] WP29, *'Future of Privacy'* (WP168) para 46; OECD, *'Towards a Culture of Security, Recommendation'* C(2002)131/FINAL 25.7.2002 no III.2.; as a duty of assessment Roßnagel/Pfitzmann/Garstka, *'Modernisierungsgutachten zum BDSG'* (German Ministry of Interior 2001) 143.
[29] EDPS, *'Trust in the Information Society'* (2010) OJ C 280/1 para 33; EDPS, *'Opinion on Area of Freedom, Security and Justice'* (2009) OJ C 276/8 para 44.
[30] EU Commission, *'Guide to the implementation of directives based on the New Approach and the Global Approach'* (EU Bookshop 2000) 9.
[31] For example the directives 85/374/EEC and 2004/35/EC create a strict liability of the producer who put defective products into circulation.

quires taking appropriate technical and organisational measures at the planning stage so as to comply with the data protection provisions. It provides for a legal compliance test and the compliance by technology users. However it lacks a legal compatibility test and a specific duty of demonstration.

Art. 23(2) requires taking technical measures in order to process only the minimum personal data that are necessary to achieve the purposes. This requirement considers in particular the claim[32] for Privacy-Enhancing Technologies (PETs). Although this data necessity criterion adds to Art. 5 DPD, the technology design aspect, it does not achieve the level of protection of the German principle of data avoidance according to § 3a of the Federal Data Protection Act. This is due to the fact that Art. 23(2) presumes that the purposes are already given, which is typical for the necessity criterion of data protection law. In contrast § 3a requires active design of the systems within the meaning of data avoidance and even to reconsider their purposes. As opposed to the necessity criterion, one has to examine whether or not one can change the given or planned circumstances of the data processing in a way that identification is not necessary anymore.[33] Using invoicing of Internet use as an example one would have to examine whether instead of an invoicing based on time or volume, the business could deploy an invoicing based on a flat rate in order to avoid the compiling of user profiles.[34] Art. 23 lacks such an optimisation requirement.

Art. 23(3) empowers the Commission to adopt delegated acts that define criteria and requirements concerning the appropriate technical measures. In particular this legal basis provides that these acts aim at adding to the general PbD provision provisions specific to sectors, products and services.

Art. 23(4) provides for technical standards that implement PbD. In contrast to the preceding paragraphs of Art. 23, this paragraph refers to "technical standards" which suggests a technology design within the meaning of technical standardisation. Art. 23(4) has prompted the author to write this paper since the references in paragraphs 1 and 2 of Art. 23 to PbD standards do not address technology producers and do not allow real technology design.

Despite these PbD standards the Commission's proposal does not establish PbD standards for automated individual decisions within the meaning of Art. 15 DPD (or Art. 20 of the draft-DPR). However, knowledge-based systems generating or preparing automated individual decisions are socially relevant. One should pay particular attention to these systems.[35] Art. 20 of the draft-DPR requires taking suitable protective measures for automated individual decisions. However, it does not make the connection to PbD and thus ignores the claim to create protection by technology design.

Even if PbD standards do address technology design one would have to back them up with duties upon the technology users who adjust the technology for their purposes. One achieves this with Accountability and PIA. With Accountability (also in Arts. 5(f) and 22) one ensures that the technology users are able to demonstrate that they have chosen and adjusted to a legally compatible technology. PIA (also in Art. 33) requires assessing how one has to choose and adjust technology.

The principle of Accountability[36] is implemented (as in Art. 5(f)) with the duty to ensure and demonstrate compliance with the data protection provisions. The demonstration adds to Art. 5(2) of the current DPD which only requires "ensuring" compliance. Accountability enforces PbD in three steps. Compliance rests with Art. 23 according to which one must undertake certain PbD measures. By Art. 22 one has to audit if appropriate the fact that one has taken the PbD measure and Art. 22(1) requires the controller to be able to demonstrate compliance.[37] This is why one needs to retain the audit report for the supervisory authority.[38] If one does not comply with one of these steps, according to the Commission, the supervisory authority would be able to impose by Art.79 a dissuasive fine on controllers. Since Accountability enables the PbD measure to be demonstrated some also regard PbD as a part of Accountability.[39] Due to Accountability it is possible to demonstrate that one chose and adjusted the technology in a legally compliant way.

On the other hand the legal notion of "Privacy Impact Assessment"[40] is relevant for identifying the choice and adjustment of technology. PbD can be enforced with PIA (also in Art. 33). This is done in two steps. First, one is obliged to assess in advance specific risks for "rights and freedoms" of data subjects that are entailed by a planned data processing activity. Second, one has to take measures to mitigate those risks.[41]

---

[32] EU Commission COM(2007) 228 final, 2.5.2007; Arbeitskreis Technik of the German data protection commissioners' conference (1997) Datenschutz und Datensicherheit 709; Borking (1996) Datenschutz und Datensicherheit 654; in computer science already Chaum CACM 2/1981.

[33] Roßnagel/Pfitzmann/Garstka, *'Modernisierungsgutachten zum BDSG'* (German Ministry of Interior 2001) 101f: *"[Es] ist zu prüfen, ob die gegebenen oder geplanten Umstände der Datenverarbeitung so verändert werden können, dass der Personenbezug nicht mehr erforderlich ist."*

[34] Dix in Roßnagel (ed), *'Handbuch Datenschutzrecht'* (CH Beck 2003) para 37.

[35] Bing in Altes et al, *'Information law towards the 21st century'* (Kluwer 1992) 247 (252); but also trivial quasi-decisions like smiling or grimacing, praising or criticising, etc. are important for the personality rights Bing (1992) 247 (258).

[36] WP29, *'Opinion 3/2010 on Accountability'* (WP173) 13.7.2010 para 34; 32nd International Privacy Commissioners' Conference, *'The Madrid Standards'* § 11; on the origin of the concept: Centre for Information Policy Leadership, *'Data Protection Accountability'* October 2009; *'Demonstrating and Measuring Accountability Phase II, The Paris Project'*.

[37] How and to whom one has to demontrate is asked by Traung (2012) Computer und Recht international 33 (40).

[38] On data protection management: Roßnagel/Pfitzmann/Garstka, *'Modernisierungsgutachten zum BDSG'* (German Ministry of Interior 2001) 131f according to which the data protection strategy (*Datenschutzkonzept*) describes how goals such as data avoidance are achieved and the strategy is kept for the supervisory authority for checks.

[39] EDPS, *'Trust in the Information Society'* (2010) OJ C 280/1 para 105.

[40] Also Clarke [2009] 25 Computer Law and Security Review 123; such a legal need for PIA is also seen by Wright, Friedewald, Gutwirth, Langheinrich, et al [2010] 26 Computer Law and Security Review 343 (344); rejecting Dutton http://people.oii.ox.ac.uk/dutton/, find blog entry with "PIA in the sky."

[41] The data protection officer is in charge of monitoring PIA (Art. 37). One can also conduct a PIA for joint applications of several controller (Rec. 72 of the draft-DPR).

PIA adds to the prior checking according to Art. 20 of the current DPD because it provides for a legal compatibility test. PIA and Art. 33 takes not only data protection into account but moreover the "rights and freedoms" of individuals as a yardstick for the assessment. That is, instead of a legal compliance test, there is a legal compatibility test within the norms of the EU Fundamental Rights Charter. Taking fundamental rights as a starting point is sensible because in relation to novel technology applications EU secondary law is full of gaps and needs to address the fundamental rights that one achieves as mentioned above, by using an interdisciplinary method.

Furthermore, PIA adds to Art. 20 of the current DPD because it does not require the result (compiling a report) but a procedure for the acceptance of technology applications.[42] In particular, this procedure includes the participation of data subjects.[43] The EU Commission suggests such a participation of data subjects in Art. 33(5).

PIA also adds to Art. 20 of the current DPD because it provides for the consultation of the supervisory authority, its power of prohibition and a duty to make proposals for improvement as well as the administrative fine mentioned above. The enforcement of PbD by PIA is strengthened because, according to Art. 34, in relation to processes with high specific risks one has to consult the supervisory authority. Furthermore, Art. 34 empowers the supervisory authority to prohibit processes as well as to make proposals for improvement. If one does not conduct the PIA the supervisory authority would be able to impose the fine mentioned above according to Art. 79.

By recognising PbD, Accountability and PIA the EU Commission contributes to choosing and adjusting technology in a legally compatible way. The proposed provisions on PIA clarify the position that one has to take as a yardstick not only data protection as EU secondary law but also the rights and freedoms of the EU Fundamental Rights Charter for a legal compatibility test. Since PIA also requires the transformation of fundamental rights for novel technology applications the EU Commission should also for PbD define the consideration of risks for rights and freedoms of data subjects. The provision on necessity in Art. 23(2) should also be concerned with the purposes of the data processing in order to enable optimisation of legal compatibility. PbD, Accountability and PIA address individual businesses and public authorities that use technology. The PbD standards that are also provided for in Art. 23(4) should also address technology producers. Besides, the Commission should also provide for PbD standards for automated individual decisions as in Art. 20.

3.2. Proposed Privacy-by-Design standards without legal method

The following subsection will submit that PbD standards are not backed up by a method that identifies the need for protection and hence the technology design. First it will describe the proposed power to adopt PbD standards. Second it will show that the provision that serves as the ground for the power lacks precision. Third it will assess the compatibility of the provision within the "new approach" of EU technology law.

Art. 23(4) enables the Commission to adopt technical standards for PbD as so-called implementing acts pursuant to Art. 291 TFEU. Such specifying legal acts are also necessary due to the dynamic development of technology.[44] The provision for legal technology design in the committee procedure is an approach already used by Art. 3 of the Directive 1999/5/EC for the production of telecoms devices and Art. 14(3) of the Directive 2002/58/EC for electronic communication.[45] Already by 1990 there was such an approach for the planned[46] ISDN Directive.[47] By "technical standards" the draft-DPR does not mean technical standards for data security - data security is subject to Art. 28 - but for the rights and freedoms of data subjects.

Further, it is not the Commission that decides what PbD standards might contain but a committee that consists of experts from the Member States. The draft-DPR opts for the assessment procedure according to Art. 5 of the Comitology Regulation 182/2011 which (unlike its predecessor pursuant to Art. 5 of the Comitology Decision 1999/468/EC) leaves it to the committee to decide. In the case of disagreement between the Commission representative and the remaining committee it is up to the committee to decide (and not the EU Council anymore) with power to refuse by simple majority the enactment of the implementing measure.[48]

It is doubtful whether the provision that serves as a ground for the power to adopt PbD standards is sufficiently precise. It is unclear how the Commission and the committee will make use of the power to adopt PbD standards.[49] The provision does not rule out the possibility that the IT experts who sit in the committee may alone decide on the privacy of citizens without legal expertise or possibly place too many limits on the marketing of innovative products by overly detailed technical specifications. Since the provision does not exclude overspecification of products it is possible that supervisory authorities might place additional limits on the freedoms of business. This can lead to barriers to trade among the Member States.[50] Providing that one has to apply a method for verifiability of PbD standards promotes foreseeability. It is an element that limits the action of the committee which promotes controllability.

With special reference to technical standardisation the EU Parliament made several demands. It claimed that one needs to "draw a clear line between legislation and [technical] standardisation in order to avoid any misinterpretation with regard to the objectives of the law and the desired level of protection." Further it demands that "the role of standardisers should be limited to defining the technical means of reaching the goals

[42] Wright [2012] 28 Computer Law and Security Review 54 (55f).
[43] Wright (2011) Ethics and Information Technology 199, 224; also Wright (2012) 28 Computer Law and Security Review 54 (58f); ICO, *'PIA Handbook'* 56 and 58; Clarke, http://www.rogerclarke.com/DV/PIAG-Eval.html, para 3.6.c.
[44] Gola (2012) Europäische Zeitschrift für Wirtschaftsrecht 332 (334).
[45] However this approach was not used yet: EDPS, *'Trust in the Information Society'* (2010) OJ C 280 p 1 para 33ff.
[46] EU Commission COM(90) 314 OJ EU 1990 C 277 p 12 (17, see "Article 21").
[47] Directive 97/66/EC.
[48] If the committee does not adopt any opinion on the draft, one can in principle enact the draft too. However the draft-DPR can also be changed in a way that this rule does not apply. Then there has to be a qualified majority in any case.
[49] See also Hornung (2012) Zeitschrift für Datenschutz 99 (103).
[50] Traung (2012) Computer und Recht international 33 (44).

set by the legislator."[51] The method for legal technology design is a safeguard that limits the PbD standards to defining the technical means of reaching the goals set by the legislator.

Using the approach of a committee procedure, one separates the legal requirement of PbD from the technical implementation. This is compatible with the EU approach for technical standardisation.[52] According to this so-called "New Approach" five principles apply in technology law. First, the legislation is restricted to the basic requirements. Second, it prohibits the marketing of products that do not meet these requirements. Third, it is presumed that the technical standards that fall within the new approach meet the legal requirements. Fourth, the implementation of technical standards remains voluntary and it is left to the producers to choose any technical solution to implement the legal requirements. Fifth, technology producers can choose from various assessment methods that are laid down in the legal instruments.[53]

The New Approach is applicable to the planned PbD standards. The legislator defines the basic requirements for technology design that promotes rights and freedoms. In relation to the prohibition of putting into circulation products that do not meet the legal requirements, the provision on PbD should as mentioned above, not only address technology users but also technology producers. The EU Commission needs also establish the presumption of conformity to PbD standards.

The voluntary nature of the PbD standards' implementation should not be pursued. One has to distinguish PbD standards from the technical standards for data security, secure signatures,[54] and product security for which the legal instruments already clearly set the goal. PbD is not so specific that it would be comparable to those goals. PbD is wider and serves the rights and freedoms of data subjects which still have to be concretised into goals. If overly detailed specifications can be referred to as goals, one requires what is legally necessary and this can and should be mandatory. The PbD standard itself should be mandatory and label examples of specifications as such.

The proposed provision on PbD standards does not itself define how one verifies whether and how a PbD standard promotes the law. In particular, it lacks a method to develop PbD standards the definition of which necessarily promotes the basic principle of foreseeability. The presumption needs to be established in line with the New Approach of EU technology law that technology producers must comply with PbD if they implement PbD standards. PbD standards should be mandatory if the method ensures that only what is legally necessary is specified.

3.3. Whole regulation proposal without legal method

If one searches the draft-DPR for a method of legal technology design, one finds the legal notion of Privacy Impact Assessment (as "Data Protection Impact Assessment" in Art. 33) which comes closest to such a legal method. As mentioned above PIA mainly defines a procedure and specifies the prior checking required according to Art. 20 DPD. The legal notion is suitable for creating the acceptance of technology applications in individual businesses and public authorities that is achieved by a procedure and in particular the participation of data subjects.

Consistently, the provision on PIA does not refer to a method of legal technology design although in practice one starts with International Organisation for Standardisation (ISO) risk assessment[55] methods.[56] Even if the PIA provision does refer to them, the ISO risk assessment methods would not be suitable because they are methods for IT security and do not address the rights and freedoms of individuals.

The need for a method for privacy-enhancing technology design became apparent during the development of the first PIA Framework.[57] Due to the fact that a method for identifying the need for protection was missing, the Article 29 Working Party (WP29)[58] had to refer to the method of ENISA – the European Network and Information Security Agency. In contrast to PIA on the level of individual businesses and public authorities, the PIA Framework deals with technology design. Therefore, it was created with the help of technology producers. Similar to the distinction between the PIA Framework of technology producers and PIA for technology users,[59] one also has to distinguish between PbD standards for technology producers and PbD for technology users. Just as the technology design by means of PbD standards cannot create actual acceptance by data subjects but only general acceptability, such is the position too with the PIA Framework.

[51] Concerning the planned EU standardisation regulation (COM(2011) 315 final): EU Parliament, *'Report on the future of European standardisation'* 7.10.2010 A7-0276/2010 no 15.

[52] EU Commission, *'Guide to the implementation of directives based on the New Approach and the Global Approach'* (EU Bookshop 2000).

[53] EU Commission, *'Guide to the implementation of directives based on the New Approach and the Global Approach'* (EU Bookshop 2000) 9.

[54] Also the Directive 1999/93/EC realises the „new approach" by providing for standardisation and voluntary accreditation; the Commission also revises that directive at the moment (EU Commission COM(2012) 238 final 4.6.2012).

[55] ISO/IEC 27005 (formerly ISO 13335-3) and sector-specific e.g. for financial services ISO 22307.

[56] Meints in Matyáš et al, *'The Future of Identity'* (2009) 298 IFIP AICT 264; similarly Büllesbach (1995) Recht der Datenverarbeitung 1.

[57] WP29, *'Opinion 9/2011 of 11.2.2011 on the revised PIA framework for RFID applications'* (wp180) 12.1.2011.

[58] As Arts. 64ff suggest, the name will change in the future.

[59] Hence PIA also seems as suitable for the legislative process in order to assess whether or not the enactment of a law is necessary: Beslay/Lacoste in Wright/De Hert (eds), *'Privacy Impact Assessment'* (Springer Dordrecht 2012); the draft-DPR also suggests this in Rec. 73f together with Art. 33; additionally the EU Commission finances a research project on PIA frameworks, http://www.piafproject.eu (de Hert et al).

The (non-legislative) PIA Framework process was prepared in several steps. An opinion of the WP29 in January 2005[60] started the process. The main follow-up measure was located in the formal beginning of the framework process by the EU Commission[61] in cooperation with the stakeholders.[62] Finally the WP29[63] adopted the PIA Framework[64] about whose implementation and effectiveness the Commission was to report in May 2012.

First the Commission specified the procedure for the process of the PIA Framework by empowering the WP29 to decide on the adoption of the result. This is relevant for the decision about a PbD standard. In the committee procedure of EU technology law it is customary that technical experts of standardisation organisations like CEN - European Committee for Standardisation and its German counterpart DIN - Deutsches Institut für Normung - as well as IT security authorities such as ENISA and its German counterpart BSI - Bundesamt für Sicherheit in der Informationstechnik - are in charge.[65] In addition the experts of individual large Member States usually control the committee work and the smaller Member States do not always appoint experts from technically competent institutions. The technical experts are not in charge for the needed legal expertise and experience; in part they even receive orders from security authorities to develop surveillance technology. In order to really promote the rights and freedoms of data subjects one should at least provide for a procedural safeguard in Art. 23(4).[66]

In addition to the procedural safeguard there is still the need for a method. The goal of the PIA Framework was to develop "guidance for the design of RFID – Radio Frequency Identification - applications in a lawful as well as socially and politically acceptable way."[67] However the Commission did not require a methodology that helps to verify whether or not the technology design actually promotes legality as well as social and political acceptability. However, the stakeholders needed such a method. This follows from the fact that the WP29, in particular, did not adopt the first draft of the PIA Framework because it did not sufficiently address the point that the technology design depends on the extent of the risks to rights and freedoms.[68] The lawyers who worked for the technology producers were not able to draft the PIA Framework alone because they could not identify the specific risks and protective measures required without an intense cooperation with engineers.

The WP29 had to remedy the lack of method. After ENISA had offered its method for the PIA Framework,[69] the WP29 made reference to it.[70] The method of ENISA builds on the ISO risk assessment method mentioned above. Despite its remarkable expansion the method chosen by ENISA is still a method of IT security that does not follow the rules of legal science. However, the goal was not data security but rather design "in a lawful as well as socially and politically acceptable way." PbD does not serve to identify technology design for promotion of data security either, but mainly the other legal goals of the rights and freedoms of individuals. Using the example of RFID applications one can illustrate this by means of the *Bundesrat's* (Upper House of the German Parliament) claim to design a label to explain how to deactivate RFID chips across the EU in a way that is simple and understandable for consumers.[71]

However, one does not have to regard the reference to ISO risk assessment methods as final but against the backdrop that the PIA Framework was the first of its kind.[72] EU-wide legal technology design has not yet been fully developed. This also becomes apparent from the fact that the EU Commission, at the same time as the PIA Framework, pursues a general approach towards self-regulation. In order to specify the opt-out rule in Art. 5(3) of the ePrivacy Directive,[73] it pursued the adoption of a best-practice recommendation of two associations in relation to online behavioural advertisements. The WP29 rejected this recommendation because it did not implement the opt-out rule.[74] In particular, the recommendation provides for the design of cookies for which the WP29 makes detailed positive suggestions.[75] Compared to this detour the PIA Framework can be seen as progress because it forces the WP29 and industry to cooperate.

Choosing the ISO risk assessment method is however only provisional and cannot ensure that technology really promotes the law, because it does not appropriately consider the input of legal expertise. Engineers cannot alone develop PbD standards since they cannot adequately follow the goals of the rights and freedoms of individuals without cooperation with lawyers. One can only achieve the technical standardisation that promotes legal goals by using a legal method of technology design.

It is submitted that not only the proposed provision on PbD but also the whole regulation proposal fails to set a method for legal technology design despite the fact that, during the PIA Framework process, it became apparent that there is a need for such a method.

[60] WP29, *'Working Document on RFID technology'* (wp105) 19.1.2005.
[61] EU Commission, *'Recommendation on PIA framework for RFID applications'* C(2009) 3200 final 12.5.2009.
[62] WP29, *'Opinion 5/2010 on the PIA framework for RFID applications'* (wp175) 13.7.2010.
[63] WP29, *'Opinion 9/2011 of 11.2.2011 on the revised PIA framework for RFID applications'* (wp180) 12.1.2011.
[64] Appendix to WP29, *'Opinion 9/2011 of 11.2.2011 on the revised PIA framework for RFID applications'* (wp180) 12.1.2011.
[65] Also in the case of the PIA Framework CEN is given a standardisation mandate, EU Commission, CEN M/436, 8.12.2008.
[66] WP29, *'Opinion 1/2012 on the data protection reform proposals'* (WP191) 23.3.2012, 8 and 11.
[67] EU Commission, *'Recommendation on PIA framework for RFID applications'* C(2009) 3200 final 12.5.2009.
[68] WP29, *'Opinion 5/2010 on the PIA framework for RFID applications'* (wp175) 13.7.2010, 7.
[69] ENISA, *'Opinion on PIA framework for RFID applications'* 1.7.2010, 1.
[70] ENISA, *' "Flying 2.0", IoT/RFID Scenario Risk Assessment'* (Final Report) 2010, 52ff; referring to that ENISA, *'EFR Framework - Introductory Manual'* 1.3.2010; in turn referring to that WP29, *'Opinion 5/2010 on the PIA framework for RFID applications'* (wp175) 13.7.2010.
[71] Bundesratsdrucksache (law gazette of the *Bundesrat*) 48/11 of 3.2.2011, 1.
[72] Poullet (2010) 11 (2) Digital magazine Dataprotectionreview.eu 1 (5).
[73] Directive 2002/58/EC as amended by Directive 2009/136/EC.
[74] WP29, *'Opinion 16/2011 on EASA/IAB best-practice recommendation'* (wp188) 8.12.2011, 3f.
[75] WP29, *'Opinion 16/2011 on EASA/IAB best-practice recommendation'* (wp188) 8.12.2011, 8ff; also WP29, *'Opinion 4/2012 on cookie consent exemption'* (wp194) 7.6.2012.

The ISO risk assessment methods and other methods of IT security that are usually applied are not suitable since they only serve to promote IT security but not the rights and freedoms of individuals. As a procedural safeguard one should specify that the WP29 is to decide on the adoption of PbD standards.

To sum up, the EU Commission, aiming to implement the principle of PbD needs to set a method and a procedural safeguard as well as an obligation upon technology producers. Further the Commission should specify that one has to consider rights and freedoms of individuals and to optimise the purposes of processing.

4. Proposal of a provision on basic properties of a legal method

The legal method of *KORA*[76] can inspire the EU legislator to introduce a provision on methods for the adoption of PbD standards. It was developed in Germany in order to implement the idea of promoting legal protection by technology design mentioned in Section 2. *KORA* is not necessarily the only method for legal technology design. It only serves as an example for such a method. Art. 23(4) or other provisions for PbD standards should only define the basic properties of the methods admissible for the adoption of PbD standards.

KORA offers the above-mentioned "bridging-approach" between law and technology and, as opposed to PIA, it is in particular suitable for designing technology on the level of technical standardisation and thus for creating acceptability. This method considers fundamental rights and other legal fundamental norms of the German as well as the EU legal order (and at least those of all other continental European countries). For this paper it is interesting to know how to apply *KORA* if the technology concerns the fundamental rights to privacy and data protection. In that field *KORA* was applied, for example, to design Internet shopping and payment, location-based services, profiles on mobile platforms, as well as e-government and e-learning in a legally compatible way.[77]

The following subsection uses as a recent example the application of *KORA* in the design of a service platform for mobile phones. This platform manages location-based services and user profiles so that users automatically receive certain information, for example, about timetables at railway stations, sights on journeys, participants at conferences, and notes for business meetings.[78]

Transforming the law into the embrace of technology is a challenge. Therefore, *provet* whose experience is drawn on, not only helped develop *KORA* but also the principle of data avoidance and data frugality. The principle of data avoidance is a classic constituent for legal technology design. Before being provided for in § 3a of the German Data Protection Act, this principle was first enacted in § 4(6) of the German Teleservices Data Protection Act[79] and § 13(6) of the German Interstate Contract on Media Services[80] in 1997 which goes back to the preparatory work of *provet*.[81] The principle of data avoidance is unique worldwide due to its connection with legal technology design.[82]

Using *KORA* one can systematically evaluate and design technical systems. After having identified the opportunities and risks of the technology, as well as the concerned fundamental rights and norms, one derives technology design proposals in four steps. These steps are referred to as (1) legal requirements, (2) legal criteria, (3) technology goals, and (4) technology design proposals. From the legal requirements one derives the legal criteria by focussing on the specific technology ("What does transparency, accountability, data minimality, etc. mean for the particular technology?"). For the technology goals one asks what basic functions the specific technology must offer to fulfil the legal criteria. From the technology goals one looks for specific technology design proposals that serve to illustrate ways to achieve the technology goals. Whereas the first two steps require knowledge in the area of the law (statutory acts, constitutional case law, etc.), the last two steps require knowledge in the area of the technology.[83] The application of *KORA* forces lawyers to cooperate with engineers.

However these four steps are not meant as setting the order of applying the method. One cannot develop a specific technology purely by means of "derivation," as assumed by legal informatics and its deductive approach. Instead one approximates the legal criteria "from both sides" until one can identify all relations between the four steps. Hence, one identifies opportunities and risks of the technology, on the one hand. On the other one looks for first design proposals that come to one's mind.[84] This way one ensures that lawyers assess the technical specific features.

Using the example of mobile profiles, location-based services and service platforms, the researchers assessed the specific features of the technology. They first examined the specific risks for the legal criteria of self-determination, transparency and use limitation. For self-determination they consider that non-explicit consent and conclusion of contract on the service platform are specific to the technology. For transparency the specific risk was the completion of the profile with data from other sources than the service platform. For use limitation, there was the specific risk of use of data on the service platform for an indefinite variety of possible services.

[76] Hammer/Pordesch/Roßnagel, *'Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet'* (Springer Verlag 1993).
[77] Roßnagel in Eifert/Hoffmann-Riem (eds), *'Innovation, Recht und öffentliche Kommunikation'* (Duncker und Humblot 2011) 54ff w.f.r.
[78] Schnabel, *'Datenschutz bei profilbasierten Location Based Services'* (Kassel University Press 2009) 3.
[79] BGBl. (German federal law gazette) 1997 I 1897.
[80] Nds. GVBl. (Lower Saxony law gazette) 1997 p 280.
[81] Bizer in Simitis, *'Bundesdatenschutzgesetz'* (6th ed, Nomos 2006) § 3a para 3; anonymous technology design for payment for telecoms services were already demanded by International Conference of Data Protection Commissioners, *'Decision of 30/08/1989 concerning ISDN'* on proposal of the Working Group Telecommunications and Media.
[82] Bygrave, *'Data protection law'* (Kluwer Law International 2002) 346.
[83] Hammer/Pordesch/Roßnagel (1993) 46f.
[84] Pordesch, *'Die elektronische Form und das Präsentationsproblem'* (Nomos 2003) 257ff.

Next the researchers examined design proposals, for example, pseudonymisation of profiles towards third-party service-providers, aggregation of the user history, and interruption of localisation.[85]

Unlike the method of IT security *KORA* follows the legal requirements of national constitutions as well as the EU Fundamental Rights Charter. Only after having legally assessed a technology can one formulate technical goals and design proposals.[86] This way one ensures that engineers develop technical functions based on legal aspects.

Using the example of mobile profiles, location-based services and service platforms, the method enabled the engineers to develop technical functions based on the law. They could build functions for "legal requirements" and "legal criteria." For the legal requirements the engineers could consider informational self-determination, confidentiality of telecommunication, as well as confidentiality and integrity of IT systems. For the legal criteria they could take into account transparency, use limitation and other data protection principles.[87]

Moreover, in contrast to conventional technical standardisation, by using *KORA* one can avoid overly detailed and comprehensive technical specifications that place too many limits on the technology producer's business freedoms, may constitute barriers to trade, and discourage innovation. *KORA* then distinguishes between technical goals and technical design proposals.[88] The design proposals describe specific technical solutions as examples for achieving the technical goals. The method also admits innovative solutions to achieve the same goals. *KORA* also avoids overly detailed specifications by describing the technical goals and design proposals as far as they are legally necessary. One does not have to describe technical solutions in every detail and completeness. It is left to technology producers to specify hardware and software for which they also have to consider non-legal aspects, as far as they implement the legally necessary technology design.

Using the example of pseudonymisation of profiles, one only defines in basic terms that the service platform centrally manages the pseudonyms in order to remove the identifiability of data towards third-party service-providers.[89] A technical goal with such an abstract formulation avoids that one (unwillingly) favours certain file formats, communications protocols, application programs, runtime environments, or operating systems.

The main added value of *KORA* is its bridging-approach for legal technology design. *KORA* is part of legal science and ensures an interdisciplinary cooperation between legal and technical experts. This is due to cooperation whereby lawyers can correctly identify the extent of the specific risks of a technology and engineers can orient their design towards legal aspects. Moreover, as a consequence of interdisciplinary cooperation, it is possible for lawyers to check whether a PbD standard really promotes the law.

Art. 23(4), or other provisions for PbD standards, should define the basic properties of the method needed for the adoption of PbD standards. This paper proposes to adopt two additional rules 1) for a legal compatibility report and 2) a five-step procedure for the technical-legal cooperation. Concerning the report the EU Commission can establish the rule that one has to adopt a report together with the technical standard. This report aims to demonstrate to what extent the standard promotes the rights and freedoms of data subjects. However, it is divided into mandatory goals and voluntary design proposals. As indicated in the PIA Framework process, the Commission can divide the procedure leading to interdisciplinary cooperation. This should aim at considering the rights and freedoms as well as technical possibilities appropriately. Accordingly, the Commission can establish the rule that legal experts and technical experts can alternatively edit the report and standard in five steps. First, legal experts can identify the specific opportunities and risks for rights and freedoms for the report as well as first technical design proposals for the standard. Then they could submit both documents to the technical experts for revision. Afterwards they can submit the revised draft to the lawyers who develop suitable legal criteria and express technical goals. In turn the engineers could revise the draft and develop technical design proposals before the lawyers agree to the draft.

5. Conclusion

Privacy-by-Design standards as "promised" by the EU Commission in Art. 23(4) of its regulation proposal offer the opportunity to make legal technology design indeed a success. They could control international standardisation and thus contribute to the improvement of data protection. One should welcome the Commission's promise to provide for legal technology design at the EU level. However, the Commission runs the risk of not keeping its promise if the provision's proposals - like now - become an open invitation for legislation that becomes subject to co-decision by the European Parliament.

In order to keep its promise the Commission should establish the procedural safeguard that the Article 29 Working Party decides on PbD standards' content. In addition, it should set a safeguard in content that does justice to the rights and freedoms pursuant to the EU Fundamental Rights Charter. The PbD committee should apply a legal method instead of leaving the protection of fundamental rights to computer science and its specification of a risk analysis. One has strictly to distinguish technical standards for IT security from the standards proposed for promotion of the individual's rights and freedoms. The method must ensure an intense cooperation between lawyers and engineers. Furthermore, the Commission should define that PbD standards not only address technology users but also technology producers because they design the technology. Diagram 1 (below) sorts these two safeguards for legal technology design into future EU data protection law and indicates in brackets where they are already laid down in law or in legal science.

[85] Schnabel (2009) 322f, 342, 344, and 360.
[86] Hammer/Pordesch/Roßnagel (1993) 45ff.
[87] Schnabel (2009) 73ff and 370.
[88] Hammer/Pordesch/Roßnagel (1993) 46f.
[89] Schnabel (2009) 324.

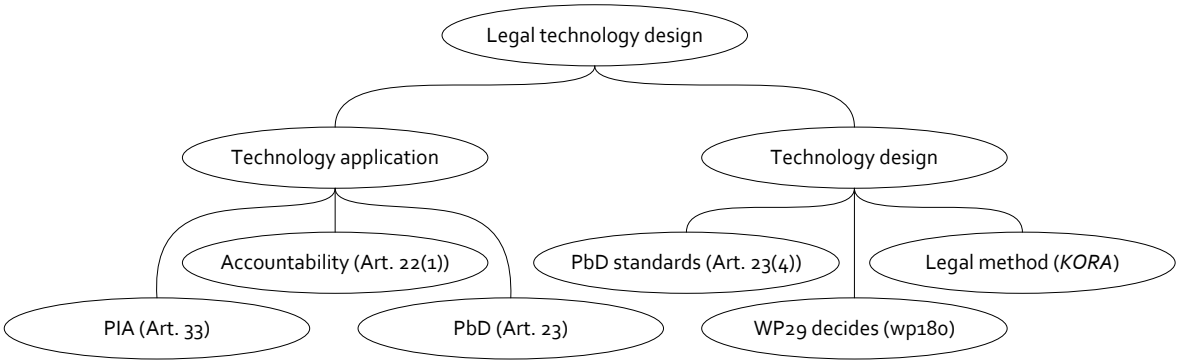

Diagram 1. Elements of legal technology design in the future EU data protection law.

We should safeguard Privacy by Design and not lose its meaning. Therefore, the Commission should establish a procedural requirement and limit the action of the committee that develops the PbD standards. The committee should apply a method which promotes the rights and freedoms of data subjects by means of technology design.[90]

[90] Everyone who supports this claim, may address the competent people's representative, eg: European Parliament, Jan Philipp ALBRECHT, Rue Wiertz 43, B-1047 Brussels, Belgium