Martin Rost, Kirsten Bock

Privacy by Design and the New Protection Goals*

Principles, Goals, and Requirements

“Privacy by Design“ congregates seven principles promising a modern pro-active approach to data protection and privacy with a global perspective. The “New Protection Goals“ claim no less than to turn data protection into a modern, proactive and operational tool by introducing six elementary protection goals which are related to each other and which are meant to be applicable universally. Whereas Privacy by Design is supported by ten Global Privacy Standards principles feeding practical needs, the New Protection Goals fall into line with the approved methods of risk analysis and protective measures such as baseline protection. Both paradigms put emphasis on privacy enhancing technologies. The authors argue to merge both approaches into a comprehensive universal concept.

1 Introduction

Privacy by Design (PbD) and the Global Privacy Standards (GPS)[1] have become a broadly accepted ingredient of European Data Protection efforts ever since the *Madrid Resolution*[2] and especially by the activities of the Article 29 Data Protection Working Party.[3] Ann Cavoukian, privacy commissioner of the Canadian province of Ontario, is recognized for years as the prime mover behind PbD.[4] She classifies PbD as a kind of sediment of experiences made globally with as yet scattered strategies and paradigms towards effective data protection. PbD is considered to be an attempt to complement the rather engineering approaches and techniques that have been developed within Privacy Enhancing Technologies (PETs) by a framework highlighting processes and their fundamental components. Protection goals and protective measures belong to the established set of tools which have been used in data security for years. The European Data Protection Directive and a few state data protection acts in Germany already know some protection goals that go beyond pure security aspects. The Data Protection Goals (DPG) or “New Data Protection Goals” fall into line with these standards and are the result of theoretical deliberations on

---

* Published in German in: DuD 2011/01, https://www.european-privacy-seal.eu/results/articles/DuD2011-01-RostBock-PbD-NSZ.pdf/view

[1] The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices – http://www.privacybydesign.ca/content/uploads/2010/05/pbd-implement-7found-principles.pdf.

[2] „ Global Privacy Standards for a Global World“ – The Civil Society Madrid Privacy Declaration, Madrid, Spain, 3. November 2009 – http://thepublicvoice.org/madrid-declaration.

[3] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp170_de.pdf.

[4] Ann Cavoukian, Commissioner@ipc.on.ca Information and Privacy Commissioner of Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario, Canada, M4W 1A8, info@ipc.on.ca.

their intrinsic classification[5] as were the practical experiences with criteria catalogues for consulting and auditing of large IT-projects[6]. The Data Protection Goals have been put into concrete requirements by a sub-group of the technical working party of the German federal and the Laender data protection commissioners to meet the specific demands of data protection.[7] They form the conceptual basis for the resolution made by the conference of data protection commissioners in Germany of March 2010 demanding first and foremost the incorporation of protection goals into a revised German Federal Data Protection Act.[8]

2 Privacy by Design

The first principle ***Proactive* not Reactive; *Preventive* not Remedial** emphasises the necessity for a proactive and also consultative rather than a merely reactive and penalising approach to data protection. This principle implicitly calls for privacy officers to participate in the design phase of new IT-projects, whether this is within their own organisation or in IT-projects in public administration. The second principle **Privacy as the D*efault*** stresses the maximum degree of privacy that can be achieved, which would be the case if each and every system is designed in such a way that in its default setting it does not (allow to) process any personal data. If a person remains inactive, he or she shall be assured that their privacy still is and will remain intact. The third principle **Privacy *Embedded* into Design** emphasises that the protection of privacy must be build into the systems in a holistic and integrative manner without diminishing its functionality. The approach is holistic, because it aims to consider from the beginning additional contexts and moreover integrates interests of the parties involved. The fourth principle **Full Functionality – Positive-Sum, not Zero-Sum** means to encourage that a reconcilement of all interests may lead to a "win-win" situation and rake in a positive-sum. It is suggested to bid goodbye to false dichotomies, such as privacy vs. data security. The fifth principle **End-to-End Security – Lifecycle Protection** emphasises the dependence of privacy on mechanisms to ensuring data security. This means for the procedural level that processes of data processing always need to be considered from beginning to end. End-to-end security in this sense does not only mean end-to-end encryption and signatures, but comprises the entire "lifecycle" of an IT-process. The sixth principle "Visibility and Transparency" is based on the necessity to verify systems and processes involved in the processing of personal data. Transparency with a view to processes and technical systems in organisations is a prerequisite for verifiability respective the ability to audit. The seventh principle is **Respect for User Privacy**. This principle settles the list of principles and forms at the same time the outset of everything that is the driving force in PbD. Yet, this principle does not merely express an appeal, but consists of yet another operative aspect and the claim that techniques should function in a user-centric way empowering the data subjects.

---

[5] Rost, Martin / Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD, 33. Volume, Number 6: 353-358.

[6] The Schleswig-Holstein audit seal for public entities and European Privacy Seal – EuroPriSe, www.european-privacy-seal.eu.

[7] The six fundamental protection goals are incorporated into the draft amendment of the state data protection act of Schleswig-Holstein as well as into the so far unpublished draft of ISO29101 - Privacy Reference Architecture, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45124

[8] http://www.datenschutz-berlin.de/.../665/ DSB_Konferenz_Entschliessungen.pdf

2.1 Global Privacy Standards

The first GPS principle **Consent** aims at a consilient consent as a requirement for the collection and use of data. The second GPS principle **Accountability** concerns responsibility, imputability, and liability for the processes of personal data processing. The third GPS principle **Purpose** focuses on the appropriation of a specific purpose. The fourth GPS principle **Collection Limitation** takes into account mechanisms of data economy, restricting the collection to a minimum, and to what is necessary for the specific purpose. Accordingly the collection of data must be fair, lawful, and limited. The rather short remarks on the fifth GPS principle **Use, Retention, and Disclosure Limitation** put forward demands concerning use, retention, and disclosure of data. Principle six focuses on **Accuracy** of data processing as it is necessary to fulfil the specific purposes of data processing. **Security**, the seventh GPS principle, gathers requirements on data security correspondent to international standards. **Openness** being the eighth GPS principle signifies the operationalisation of transparency as a prerequisite to accountability and responsibility for data processing. It is demanded that information about policies and practices relating to the management of personal information should be readily available for interested individuals. The ninth GPS principle **Access** requires to provide access for individuals to their personal information and to inform them about its use and disclosure. The individual should be in a position to either confirm or deny the accuracy and completeness of the information. Finally, the tenth GPS principle **Compliance** of organisations requests that organisations take the necessary steps to monitor and evaluate their processes, guidelines, and policies with respect to privacy.

2.2 Diskussion PbD / GPS

Perusing the principles and requirements one comes across only a few surprises: Proactive data protection is for many privacy officers in Germany if not a common, a targeted practice for at least ten years. Privacy by default is known in data security as a classic “firewall strategy” (one sets out closing all ports and continuous to open only the ones that are needed). With respect to market realities as well as to the relationship between public administration and citizens, this is considered an unrealistic maximum performance.[9] It shows the difference between a north American understanding of privacy as a “defence right” (Spiros Simitis) and the European data protection concept of modelling necessary communication, even if considering the principal role consent plays in the concept of fair-practices in PbD/GPS. The principle of privacy build into technology is the paradigmatic heart of Privacy Enhancing Technologies (PETs), a concept known for about ten years in Germany and the EU. The fourth principle promises the chance of a non-zero-sum situation if organisations take heed of data protection. The economic evidence that data protection pays off is indicated by the increasing number of privacy audits and certifications over the past years, not only in Germany. The principle of end-to-end security rather addresses not a classical security measure but a call to system designers to take into account termination when starting to initiate a process.

[9] Albers, Marion, 2010: Grundrechtsschutz der Privatheit; in: Deutsches Verwaltungsblatt, Vol. 17, 2010: p. 1068.

Interim conclusion: PbD can be understood as “PETs plus privacy enhancing processes”. These are not new components, but rather state-of-the-art of a modern understanding of which components should be included in effective data protection. This is why the PbD principles should receive more attention in Germany and Europe and should be integrated into existing concepts. The additional value of PbD is from our point of view to explain and clarify that data protection and privacy are “social” projects that can neither be separated nor dissolved into data protection and data security technology. Law and technology react on antecedent, latent conflicts deriving from the structure of a society. Many and also professional privacy activists have lost track of this aspect antecedent to the law when they stop all activity, anticipating this to be a professional habitus once they are presented a legal basis and yet, the substantial problem continues to exist. And secondly, with the potential to reach global consent PbD unites the essential components for effective data protection across boarders and in world society.[10]

A relevant résumé concerning the “Privacy by Design”[11] approach is drawn by Simon Davies (London School of Economics & Privacy International). For Davies PbD represents a sense of evolutionary developmental logic along the line of data protection challenges posed since the 70s. Inter alia, he points out that “Privacy by Design” reacts to the provocation by “Surveillance by Design” that was discussed in 1994 within the framework of the “Communications Assistance for Law Enforcement ACT (CALEA)”. Davies notes that the intentions of PbD date back to the 90s and are already deeply anchored in encryption techniques or even PETs and lists respective technologies that follow the PbD principles. Davies conclusion is: PbD is more a mutual consent concerning the challenges of data protection rather than presenting the targeted technical solutions. He argues that PbD offers a significant overlap between two domains, the regulative and the engineering, and the principles could be motivating; yet, they would rather fit into the regulatory horizon. They are offering too less technical substance and not enough connection points for economical interest. The seven principles are motivating and inspiring, but according to Davies do not show the potential for all interested parties.[12] Technically convertible principles need to be specifically tailored. This critical point stressed by Davies, is exactly where, as we believe, the New Protection Goals come into play.

3 The New Protection Goals

Working with protection goals is familiar to most IT-security officers: For many years protection goals have been listed in catalogues, their coverage has been commented and finally measures for their attainment have been lodged. Working with them proved successful. They are formulated in a way as to meet the demands of technical and organisational systems both in an abstract overview and in a comprehensible form of sufficiently concrete measures. The “classic” protection goals

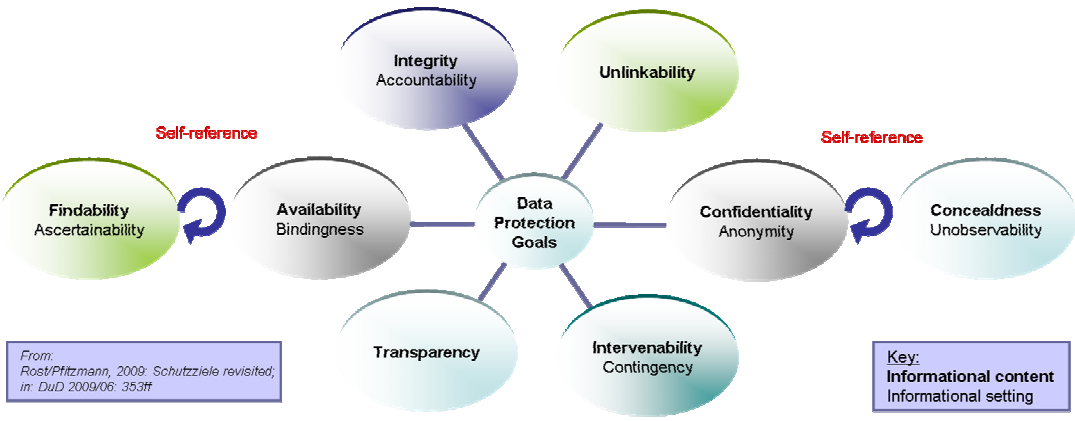
[10] Rundle/Glueck have condensed 10 „Data Protection Principles“ from sources around the world (a.o. APEC, OECD, FTC, EU-Directive), that should also be considered more closely. http://www.microsoft.com/mscorp/ twc/endtoendtrust/vision/lop.aspx

[11] Davies, Simon, 2010: Why Privacy by Design is the next crucial step for privacy protection – A discussion paper, (Stand: 2010-10-27) http://www.icomp.org/blog/wp-content/uploads/ 2010/10/privacy-by-design.pdf

[12] Cf. Davies 2010: 4.

of data security, that are **availability, integrity, and confidentiality** focus primarily on such demands that are made to guarantee the safe and secure maintenance of operation and infrastructure of an organisation. Data protection in contrast specifies these demands focused on organised data security primarily from the perspective of personal data of subjected individuals (more precisely: Citizens, customers, users, and patients) and augments this perspective with further specific demands derived from superior basic rights of individuals. The specific demands can likewise be shaped into protection goals. The specific data protection-protection goals are **transparency** – as a prerequisite for governance and regulation of technical-organisational processes as well as for weighings related to the purpose of data processing, necessity, data thriftiness, information needs of the data subjects and so on – **unlinkability** – as an operationalisation of purpose bindingness/purpose separation – and the **ability to intervene** – to operationalise especially data subject rights and the ability of information processing entities respective operators of systems to demonstrate verifiable that they actually have steering control over their systems and are not dominated by the system. These six protection goals are backed by protective measures.

The measures concerning the three classic protection goals of data security are well known. To assure availability, the redundancy of available systems is increased or sophisticated fallback and/or patch strategies are at hand. Securing integrity usually implies well organised hash-value checks. And confidentiality of databases or communication is provided by differentiation and segmentation and especially by encryption techniques. In most cases these measures are to be specified more closely with regard to data protection requirements. Classification and methods to modulate systems to determine the protection needs of data (which are thereafter inherited by the system) for risk analysis and risk handling are similarly known – and in a way exemplary for a systematic handling of data protection risks. The specific protection measures for data protection can than be fitted into this methodology.



3.1 Protection Measures

The protection goal **transparency** meaning more than mere “assessability” is to be established by measures that guarantee that the collection and processing operations of data and its use can be planned, reproduced, checked and evaluated with reasonable efforts. In this sense these measures contain a methodological

project management including a step-by-step test and release mechanism; *documentation* of IT-infrastructure of processing operations, of the data and the data flows, the security measures including the *information* of the data subject and possibly the composition of a “data letter”. In its orchestration the entities, data and operations involved in a process need to be planned beyond legal boarders, controlled in the sense of a monitoring, and logged to analyse and verify. A so called quick-freeze of a data processing operation (comprising the whole process or single incidents) needs to be possible to assess the system status at all times.

The data protection goal of **unlinkability** is meant to operationalise purpose bindingness and purpose separation. Purpose bindingness always requires the knowledge of those thematically related processes against which the predominant purpose is to be segregated to allocate and determine the logic and necessity to link data or sub-processes under a specified purpose. Unlinkability is to be implemented by such measures which guarantee that the data of a processing are not to be collected or only with excessively high efforts, processed or used for another than the designated purpose. The measures package to achieve this goal mainly includes role and architecture concepts. This entails in detail at least reasonable *separations of functions and roles* in and between organisations encompassing responsibility assignments to competent employees; a controlled *conception*, implementation, configuration, activation and decommissioning, testing and simulation in the respective phases according to best-practice terms; the deployment of *techniques* which entail *loosely coupling* or narrowly tailored services (meta directory, federation services, service oriented architectures, etc.); the *control of regulated processes* to collect, use, delete data using up-to-date techniques.

The protection goal of **intervenability** can be achieved by measures that allow the user to exercise his or her entitled rights. In consequence this means to provide an operative access to processes and data. It can amount to the establishment of a single point of contact (SPOC) for data subjects to address an intervention including traceability options. Data subjects must have the opportunity to gain access to data in running operations which must allow access, change, correction, blocking, and deletion. Transparency therefore would require for example that it can be proven to the data subject that a deletion of data initiated by the data subject actually includes all generations of copies and backups. Within the IT-design processes need to be arranged respectively separated in a case-related way so that any intervention or system failure may not have system-wide effects, nevertheless at least parts need to be excluded from the production. It makes sense to implement fine granular instead of blanket consent for the processing as well as time limited consent. It would be desirable, because consequent, to install *personal agents within IT-organisations* whose task would be to monitor the processing in the interest of the data subjects and who would be equipped with informational and agency tools. It would be the task of independent external supervisory entities to check such agents whether they comply with legal obligations and whether they balance the interests of the data subjects and organisation appropriately. From the six fundamental protection goals further goals can be deducted; they are shown in the table but cannot be further elaborated here.

3.2 Operationalisation of Trust

The basic principles that operationalise the protection goals are essentially two:

1. They operationalise the general societal requirement that system operators must be able to keep their systems under control as part of a social infrastructure and are able to prove this.
2. Protection goals operationalise the requirements applied to any system design facilitating its fair use by all parties involved.

Fair use in this context first of all refers to a binding and compulsory orientation in line with the regulatory framework which if in doubt needs fair interpretation, too. The realization of both principles is a prerequisite for all actors to reasonably trust in the correct functioning of controlled systems or respectively in the fairness of society-wide implemented infrastructure. Trustworthiness enables fast communications. This is a fundamental characteristic of modern societies. The attestation of controllability of systems is - different from fair-practice - an aspect that did not play a significant role in PbD yet, however it can deducted logically. The six basic goals enable us to phrase requirements for any processing that is to be conceptualized for three different domains in which different types of PETs can be used in correlation to each other.

4 Three Process/Operation Domains

Whenever ubiquitous computing becomes a reality – and the Internet accompanied by smart phones and devices already is such a reality -, this reality, giving organisations already an operative edge towards the individual, should also work to the advantage of the user. A technically mature and privacy friendly communication infrastructure requires at least three components which we count among the process domains' operative elements: A program which activities are solely under the control of the user in the sense of a personal "Identity Protector" (John Borking), and also an IT-based *data protection management* for organisations which serves a *user-controlled identity management type 3*[13] as well as the interest of organisations. These two process domains, at one point under the control of the user and at one point controlled by the organisation, are then attached to a third process domain, namely a basal *societal information processing and communication infrastructure*, for which the Internet and its services is paradigmatic. This infrastructure must, in an analogy to road traffic, demand that it is available to each and everyone in a society-wide neutral way, without asymmetries in power in favour of organisations, as an operative prerequisite of fair market conditions, rule of law and open truth discourses.

A **user-controlled identity management** (ucIM) is basically supporting a differentiated utilization of different types of pseudonyms.[14] A respective programme offers pseudonyms such as one time use transaction pseudonyms, anonymous credentials, and unlinkable pseudonyms such as used in the new German identity card ("Neuer Personalausweis"), as well as role- and relational pseudonyms all the way to personal pseudonyms. There aim is to reduce the likelihood and risk posed by organisations to link various user activities. However, the condition for a really

[13] Meints, Martin / Zwingelberg, Harald, 2009: Identity Management Systems – recent developments; http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf

[14] Hansen, Marit / Pfitzmann, Andreas, 2010: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version v0.34 Aug. 10, 2010,http:// dud.inf.tu-dresden.de/literatur/Anon_ Terminology_v0.34.pdf.

effective use of pseudonyms in the Internet is that the communication infrastructure allows anonymous communication relationships. It is decisive in this respect that the user, for the purpose of the protection goal of intervenability, is in control of whether to expose the rules which govern the matching between the pseudonym and his or her genuine personal data. Above this, any application for identity management should be able to control possibly personal agents and should as well provide for consent management in the context of existing communication relationships.

In the area of **organisation-internal data protection management** there has been some movement since 2007 in the wake flow of ISO27001 (Information security Management) and the ITIL-paradigm (with regards to the coordination of the interface between an organisation and technology) and standard procedures. Data protection at this is applied to all standardized procedures. Plus, one can detect increasingly more efforts to appraise and approach incidents in incident, problem, and change management not only with respect to data security but also to data protection and privacy. Here too, the new protection goals prove extremely useful. It is, however, important to provide an anchor for user controlled identity management on the organisations level in the sense of an “enterprise controlled identity management” (ecIM). Such a development is expected to take place in Germany en passant in the context of adapting workflows to the requirements set out for the issuance of certificates for organisations to be allowed to access the eID function of the new German identity card. It shows, that in many cases of interaction between organisations and individuals it is absolutely sufficient for individuals to authenticate themselves by using a pseudonym. A full identification only becomes necessary in some constellations involving the sovereign or where there is a credit risk for a corporation. A fundamental element of data protection management consists in it being controlled, regulated, and governed by the management just like all other processes in an organisation. This involves for example for processes with data protection measures and in order to increase transparency and intervenability, to create so called key risk performance indicators (kpi) or even better key risk indicators (KRI)[15]. Here, an automated support would not only be desirable but inevitable. The challenge now is to examine whether a renaissance of basic automation approaches, pursued firmly for the first time in P3P[16] (in ucIM/ecIM) and EPAL[17] (in organisational data protection management) is a possibility.

The **social data protection infrastructure** into which the other two process domains are integrated covers society-encompassing incentive, sanction, political, and academic discourse and reflectance infrastructure. The instrument of a voluntary external audit of companies and services is part of the incentive structure which enables market participants globally to signalise that they are offering outstanding data protection in their products and services. The data protection goals are relevant as well for the audit process itself - which in itself has to comply with requirements respective transparency (in publicly accessible criteria catalogues and summary minutes), integrity (proficiency, financial independence, and impartiality of the certification body), and purpose (compliance plus) - but also to the fact, that protection goals and their measures are naturally an integral part of the audit criteria

[15] An overview including various documents on different controlling paradigms and instruments in CoBIT and ITIL can be downloaded at http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx.
[16] http://www.w3.org/TR/P3P/.
[17] http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

catalogue. The focal controlling function from a data protection point of view in an external audit is that from the organisation financially independent entities evaluate with the help of competent experts the processes of organisations whose data protection risks are or cannot be estimated by the individuals affected (data subject) or were corporate trade secretes or security interests of organisations are involved.

5 Conclusion

The concept of the new protection goals which to be sure is process-oriented and based on PET does not only incorporate the principles and requirements of Privacy by Design and Global Privacy Standards comprehensively, but also eliminates the shortcomings with regard to the ability to integrate regulatory, technical, and business demands as identified by Simon Davies for a modern and globally feasible data protection concepts. The new protection goals in conjunction with modern audit instruments bring into focus not only fairness, but also the ability to control (and thus verifiability) of systems. (Protection-) goals may be targeted from different starting points. Whether they were achieved is not alone controllable by definite protection measures but further measurable by kpi/kri! And thus, they are legally, economically and technically assessable. The ability to control is a requirement for operating data protection processes. It is quite plausible to apply the same protection goals to three differently-handled data protection process domains which are distinguishable in the structure in which control is performed:

- User-controlled identity management
- Data protection management of an organisation (process control)
- Data protection infrastructure of a society including organised advise, audit, and inspection structures.

By implementing the protection goals the national as well as the European data protection regulations and the principles and requirements of PbD/GPS can be accomplished comprehensively.

Kirsten Bock
Head of EuroPriSe – European Privacy Seal at Unabhängiges Landeszentrum für Datenschutz (ULD) in Kiel, Germany.
E-Mail: kbock@datenschutzzentrum.de

Martin Rost
Senior Adviser for „System Data Protection“ at Unabhängiges Landeszentrum für Datenschutz (ULD),
E-Mail: martin.rost@datenschutzzentrum.de