IDIS (2010) 3:253–255
DOI 10.1007/s12394-010-0061-z

Privacy by design: delivering the promises

Peter Hustinx

Received: 7 January 2010 / Accepted: 16 April 2010 / Published online: 7 May 2010

Abstract An introductory message from Peter Hustinx, European Data Protection Supervisor, delivered at Privacy by Design: The Definitive Workshop. This presentation looks back at the origins of Privacy by Design, notably the publication of the first report on "Privacy Enhancing Technologies" by a joint team of the Information and Privacy Commissioner of Ontario, Canada and the Dutch Data Protection Authority in 1995. It looks ahead and adresses the question of how the promises of these concepts could be delivered in practice.

Keywords Privacy-enhancing technologies · Privacy by design · Data security

The concept of "Privacy by Design" is closely related to the concept of "privacy enhancing technologies" or PET. This term was used for the first time in the report "Privacy-enhancing technologies: the path to anonymity" that was published in 1995.

This report was the result of a joint project set up by the Dutch Data Protection Authority and the Ontario Information Commissioner. It explored a new approach to privacy protection, with a number of case studies to show that systems with no personal data—or at least with much less personal data—could have the same functionalities.

Two deputy commissioners—Ann Cavoukian at the Canadian side and John Borking at the Dutch side—played a key role in this project. The report was published in North America and Europe on the same day, and subsequently presented at the International Conference of Data Protection and Privacy Commissioners in Copenhagen.

* * *

If we now—more than a decade later—take stock of the progress made, it is only fair to say that the concept of "privacy enhancing technologies" has been fully accepted. In some ways, it is considered as a strong trademark, and there have been different attempts to benefit from its reputation and include other technologies, that are not necessarily "privacy enhancing", but "privacy enforcing" or "privacy enabling".

P. Hustinx (✉)
Brussels, Belgium
e-mail: peter.hustinx@edps.europa.eu

It is also clear that the concept of PET is closely related to the principle of "data minimization" that is now widely used, and gradually developed into the principle of "Privacy by Design" that is not only relevant for information technology systems, but also for organizations and methods in general, and thus also for "more effective" data protection authorities.

A number of countries have invested in a better understanding and promotion of PET. Notable examples are Canada, Germany, the Netherlands and the United Kingdom. The European Union's Seventh Framework Program for research and technological development (FP7)—the EU's chief instrument for funding research over the period 2007–2013—also emphasizes the importance of "building in" privacy safeguards in technological solutions.

However, at the same time, we can observe a disappointing lack of progress in the uptake and practical use of PET in relevant areas. This is probably also due to a lack of incentives, or in any case sufficiently strong incentives, to include PET in main stream projects. This is why the European Commission will be organizing a workshop on the economic benefits of PET on 12 November 2009 in Brussels, only a few weeks from now.

This means that apart from continued promotion activities, we need to invest in clarifying—and where necessary increasing—incentives for the practical implementation of PET.

* * *

Against this background, let me mention five points that in my view could make a decisive difference in this respect.

First of all, it should be clear that the need for "Privacy by Design" could never be better illustrated than by the increasing number of data security breaches that we have seen in recent years. As far as Europe is concerned, this is not only true for the UK, but also for other EU member states. In fact, security breaches may well be a structural problem for an information society that is increasingly dependent on the good performance of ICT. This should therefore also be seen as an opportunity for "Privacy by Design".

Secondly, it should be noted that present legal frameworks already impose an obligation to implement PET in some "high risk" areas. This is certainly the case for Article 17 of Directive 95/46/EC, which requires *appropriate technical and organizational measures* to protect personal data against *all unlawful forms of processing*. This is of course highly relevant for e-Health, e-Government and similar areas.

Thirdly, it seems to me that specific rules could be envisaged to impose "privacy by default" settings in a number of areas, such as RFID-applications and social networks, if voluntary measures would not be sufficiently effective. This would also apply to "cloud computing"—in any case for individual consumers.

Fourthly, it would be important to introduce the principle of "accountability" as laid down in the proposal for International Standards prepared by the Spanish Data Protection Authority. It would mean that a responsible organization should be able to *demonstrate* compliance with its data protection obligations. This would stimulate the use of Privacy Impact Assessments and Privacy Audits, and would shift the balance in privacy compliance.

Finally, it would be important to include the principle of "Privacy by Design" among the basic principles of data protection, and to extend its scope to other

relevant parties, such as producers and developers of ICT products and services. This would be innovative and require some further thinking, but it would be appropriate and only draw the logical consequences of a promising concept.

* * *

Let me emphasize that none of these points would require undue efforts or imply unfair burdens. All of these points would help to ensure that the promises of PET and "Privacy by Design" are delivered in practice.