W3C Workshop on Privacy and data usage control

Position Paper Deutsche Telekom, Group Privacy

Frank Wagner

Deutsche Telekom AG
Service Headquarters, Group Privacy
Deutsche-Telekom-Allee 7, 64295 Darmstadt, Germany
frank.wagner@telekom.de
www.telekom.com

Version: 1.0
Stand: 10.09.2010
Status: final

public

1 Data privacy at Deutsche Telekom

The protection of personal information has top priority in the Deutsche Telekom Group. Deutsche Telekom has introduced a range of measures to improve data privacy.

2008 was an exceptional year in terms of data privacy at Deutsche Telekom. The Group was confronted with incidents with far-reaching consequences for our customers' trust and therefore the general perception of Deutsche Telekom among the public and its customers.

Some of these incidents fell within the scope of criminal law and concerned the very sensitive area of personal communication – one which is officially protected under the secrecy of telecommunications. As urgent action was needed, a new Board of Management department - Data Privacy, Legal Affairs and Compliance - was set up in October 2008 and Dr. Manfred Balz appointed the Board of Management member responsible for it. This embedded data privacy and data security at the highest management level, a step which considerably increased awareness of these issues within the company.

2009 was a year of change for data privacy. In addition to rapid and comprehensive handling of the known data incidents, new structures were also created and numerous technical and operational measures put in place to improve data privacy within the company. Deutsche Telekom also became the first DAX-30 company in Germany to publish a data privacy report in May 2009, now scheduled to be published annually, to make the issue of data privacy at Deutsche Telekom transparent to the public. The goal of all these efforts is to establish a culture that reinforces data privacy for the long term. Deutsche Telekom will continue to push this process ahead in the coming years.

2 Integrating data privacy in development processes

Implementation of the aforementioned measures further improved the processes for involving the Group's data privacy organization. Early, mandatory involvement at the development stage and as new product ideas are first firmed up builds in a high level of "privacy by design" by ensuring that certain budget-relevant management decisions in the course of our development processes are not taken without the involvement of Data Privacy. Approval from Data Privacy is needed before any product can be launched. The following diagram shows the development phases, the different intensity levels of project support, which are set at the start depending on the sensitivity of the individual project, and the decision points in between.

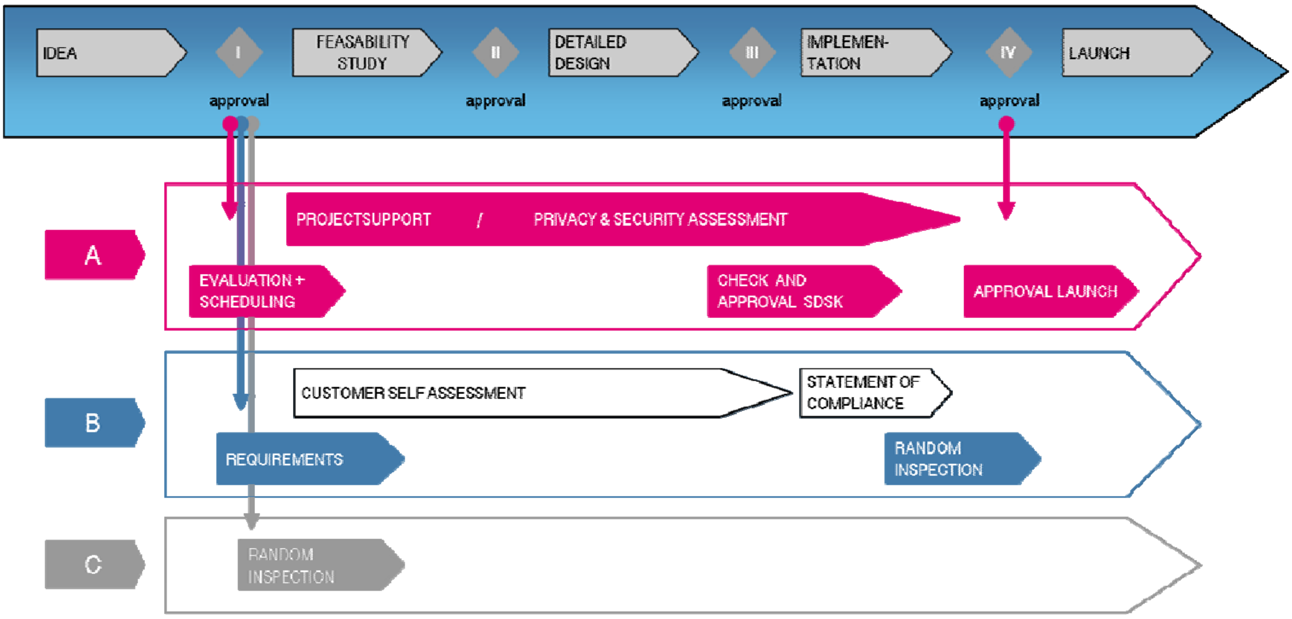

Figure 1 - Operating model

3 Solution-oriented advice – privacy by design

When providing advice on aspects of data privacy law, it can generally be said that the ability to exert influence declines as the development phase progresses. The early integration of Data Privacy in product and service design processes as described alters the demands placed on this advice.

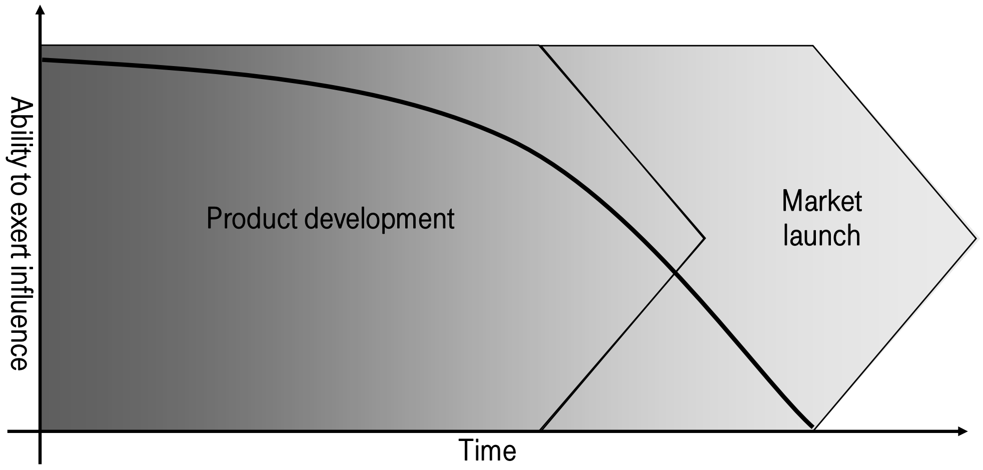

Figure 2 – Ability to exert influence

In the past it was issues such as the legal legitimization of the collation, use and processing of personal data that tended to dominate the data-privacy side of product design. Involving Data Privacy in projects from the start gives us greater opportunity to formulate the requirements for the projects that may have a major influence on the design of products, right down to fundamental aspects of their architecture. The major complexity of existing data processing systems used to provide services and design products has to be taken into consideration just the same as the manifold opportunities to link up personal data from the usage of products via the Internet. In certain cases the current scope for influencing the handling of personal data is inadequate. In networked scenarios in particular our scope of opportunity is limited to giving users tips on handling their data. We are unable to offer specific technical solutions for some kinds of problems.

The following examples from our day-to-day experience demonstrate this problem.

3.1 Synchronizing address information from social networks

One of our products lets users synchronize contact information from various sources (e-mail client, cell phone, etc.) with an address book on the Internet. A function has now been added to this product that allows data from address books on social networking sites to be synchronized, too. For the first time it was possible to add data from other sources directly; whereas the user previously had to enter the information in the address books by hand, it was now possible to create simple links.

The aspect of processing and using personal data such as e-mail addresses, cell phone numbers and postal addresses has changed so that members of a social network now not only reveal their details to other members, but – depending on the conditions of the network (terms & conditions, privacy statement, etc.) – are also opening them up to processing on third-parts systems outside their control.

This gives rise to the problem that if a user withdraws the release of his/her data, any data that is already outside the confines of the social network can still be used, although this may be against the wishes of that user.

3.2 Linking phonebook entries with geodata

Online phonebooks link addresses with city maps as well as satellite and aerial photos if customers do not object.

This right to object is mentioned in the notes on data privacy.

This behavior is made legitimate by the fact that the customers in question – in exercising their right of self-determination over their own data – have decided to publish their name, telephone number and address in "public directories" on the Internet.

In general, there is no easy way to block access to map material in the case of well-known addresses. It's always possible to find well-known addresses via other Internet services (Google maps, bing maps, route planners).

In areas that fall within Deutsche Telekom's responsibility, therefore, customers are offered the opportunity to deactivate direct links within the portals. Effective protection against disclosure of the address in the relevant map material on the Internet could only be provided by refusing publication of the address in all public telecommunications directories. Depending on the individual needs of the customer, this is not always an adequate solution.

4 Expectations of the workshop

We expect participation in the W3C Workshop on Privacy and data usage control to give insight into the design mechanisms currently available and under development that we can use in future product developments. We would be very happy to contribute our practical experience to the discussion and look forward to a creative exchange of ideas. The goal should be to find mechanisms that make it possible to control data streams in networked scenarios with decentralized responsibilities. This kind of technology is an important element in making sure the design of products, services and systems conforms with data protection requirements.