# Making Privacy by Design Concrete

Jaap Henk Hoepman, The Privacy and Identity Lab, Radboud University

**Privacy by design is a system development philosophy that says that privacy should be taken into account throughout the full system development lifecycle, from its inception, through implementation and deployment, all the way until the system is decommissioned and no longer used. In software engineering terms this makes privacy, like security or performance, a software quality attribute or non-functional requirement.**

Privacy by design is relatively well understood for the actual design and implementation phases of the software development lifecycle (Figure 1). For these privacy design patterns and privacy enhancing technologies help the engineer moving forward. For the concept development and analysis phases privacy by design is less well understood. There are of course privacy impact assessments, but these typically assume a proper design of the system, whose privacy impact needs to be assessed, is available already. A catch-22 situation, really.

To make privacy by design concrete for the early stages of software development as well, we developed eight privacy design strategies. These strategies translate fuzzy legal norms into more concrete design goals that are easier to work with for designers during the concept development and analysis phase of the system development process.

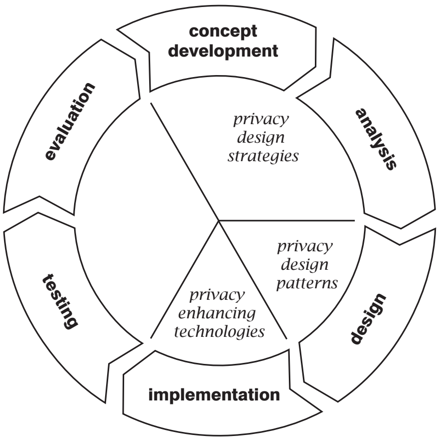

Figure 1: System development lifecycle

31

Researchers steal data from CPU cache shared by two VMs.

These design strategies offer talking points to discuss how the system could be designed in a more privacy friendly fashion, using the approach described by the strategy under consideration. The idea is to consider all strategies, one after the other, and not to focus on a single one only. Applying each strategy in turn will deliver a set of design choices that will improve the overall privacy protection of the system being designed. Which strategy is most fruitful in returning useful design choices depends on the particular system being designed.

We have identified eight such privacy design strategies (Figure 2), by studying the ISO 29100 Privacy Framework, the Organisation for Economic Co-operation and Development (OECD) guidelines and most importantly the General Data Protection Regulation (GDPR), which mandates privacy by design, and which comes into force May 2018. The first four privacy design strategies are data oriented: they focus on minimising the privacy impact of the data processing itself.

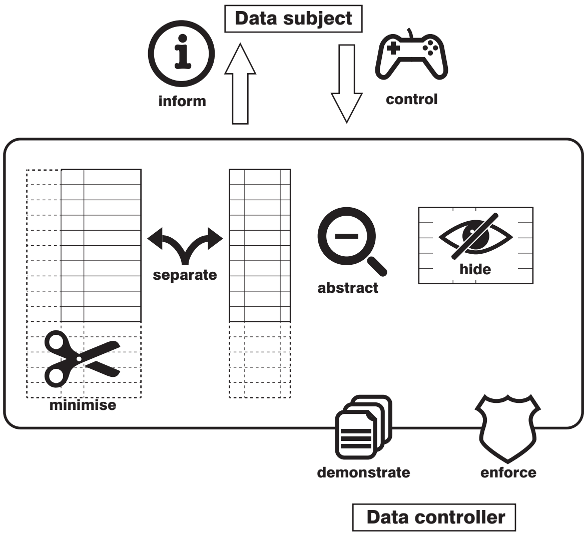

Figure 2: Eight privacy design strategies

## Minimize
Limit the processing of personal data as much as possible. There are several ways to achieve this. You can exclude information that is certainly unnecessary. You can only select information that you know you certainly need. You can strip unnecessary data as soon as it is no longer needed. And you can destroy any remaining data as soon as possible.

## Separate
Prevent correlation of personal data by separating the processing logically or physically. Logical separation can be achieved, for example, by defining different database views. Physical separation can be achieved by distributing the processing of data over separate databases. A more extreme approach is to move from a client-server model to a peer-to-peer model of processing, where personal data is processed in the endpoints (in other words the devices like smartphones owned by the users themselves).

## Abstract
Limit as much as possible the amount of detail of personal data being processed. For example, by summarizing data (like storing someone's age instead of the exact date of birth) or grouping data (like processing data about a group of people all living in the same area, instead of each of them individually). Also, one can perturb data by adding noise to it, like reporting only approximate locations for location based services.

## Hide:
Protect personal data, or make them unlinkable or unobservable. Prevent personal data from becoming public. Prevent exposure of personal data by restricting access, or hiding its very existence.

The other four strategies are process oriented: they concern the interface with the data subject and the data controller, and focus on the processes required to implement proper privacy protection there.

## Inform
Provide data subjects with adequate information about which personal data is processed, how it is processed, and for what purpose. Provide essential information in an easy to understand manner (for example using icons), but also provide pointers to more extensive background information. When relevant, provide real-time notification of data processing (for example the arrow notifying iOS users of the use of their location).

## Control
Provide data subjects with mechanisms to control the processing of their personal data. Allow them to update or even retract their personal information. Ask for consent (and allow it to be withdrawn) where relevant. Provide a meaningful choice, allowing users to access a perhaps limited functionality if they do not consent to share their personal information.

## Enforce
Commit to a privacy friendly way of processing personal data, and enforce this. Create a company-wide privacy policy, update and enforce this but most importantly uphold it by assigning clear responsibilities and supporting those with adequate resources. Think about implementing a privacy management system

**Data Oriented**

Minimise

*Limit as much as possible the processing of personal data.*

Separate

*Distribute or isolate personal data as much as possible.*

Abstract

*Limit as much as possible the detail in which personal data is processed.*

Hide

*Prevent personal data to become public or known.*

**Process oriented**

Inform

*Inform data subjects about the processing of their personal data.*

Control

*Provide data subjects control about the processing of their personal data.*

Enforce

*Commit to processing personal data in a privacy friendly way, and enforce this.*

Demonstrate

*Demonstrate you are processing personal data in a privacy friendly way.*

**Figure 3: Summary of the eight privacy design strategies**

similar to an Information Security Management System (ISMS) from ISO 27001.

## Demonstrate

Maintain evidence that you process personal data in a privacy friendly way. Do this by logging critical actions, auditing your systems and activities, and reporting on this.

Using these privacy design strategies in your system development process should make privacy by design more concrete. At least it will make it easier for system engineers to think about designing privacy friendly systems using concrete concepts they are familiar with, instead of the underlying legal concepts that offer them little guidance.

## More information

G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design - From policy to engineering. Technical report, ENISA, December 2014. ISBN 978-92-9204-108-3, DOI 10.2824/38623. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering – IWPE'16, San Jose, CA, USA, May 26 2016. http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf

April

10

ISOC tells G20 nations: The web must be fully encrypted.

BrickerBot targets Linux based IoT devices.