
PbD
Privacy by
Design

Privacy by Design Agenda

- Background
- Strategies
- Tactics

Background

- GDPR – companies were not ready
- Methodologies for translating legal requirements to software requirements do not exist.
- PbD lacks concrete:
  software tools & mapping guidelines
- Privacy patterns (SW design patterns)
- Privacy design strategies

Strategies

- Privacy design strategies provide a potential bridge between legal and engineering domain.
- Original definitions are broad and vague
- Attempt to redefine them more concretely

Tactics

- Approaches to PbD
- Comprehension
- Classification

Strategies by Tactics

MINIMIZE	HIDE	SEPARATE	ABSTRACT
EXCLUDE SELECT STRIP DESTROY	RESTRICT MIX OBFUSCATE DISSOCIATE	DISTRIBUTE ISOLATE	SUMMARIZE GROUP
INFORM	CONTROL	ENFORCE	DEMONSTRATE
SUPPLY NOTIFY EXPLAIN	CONSENT CHOOSE UPDATE RETRACT	CREATE MAINTAIN UPHOLD	AUDIT LOG REPORT

Minimize

- **Minimize**: limiting usage as much as possible by excluding, selecting, stripping or destroying any storage, collection, retention or operation on personal data, within the constrains of the agreed upon purposes.
- Tactics:
- **Exclude**: refraining from processing a data subject's personal data, partly or entirely, akin to blacklisting or opt-out.
- **Select**: decide on a case by case basis on the full or partial usage of personal data, akin to whitelisting or opt-in.
- **Strip**: removing unnecessary personal data fields from the system's representation of each user.
- **Destroy**: completely removing a data subject's personal data.

Hide

- **Hide**: preventing exposure as much as possible by mixing, obfuscating, disassociating or restricting access to any storage, sharing or operation on personal data, within the constraints of the agreed upon purposes.
- Tactics:
- **Restrict**: preventing unauthorized access to personal data.
- **Mix**: processing personal data randomly within a large enough group to reduce correlation.
- **Obfuscate**: preventing understandability of personal data to those without the ability to decipher it.
- **Dissociate**: removing the correlation between different pieces of personal data.

Separate

- **Separate**: preventing correlation as much as possible by distributing or isolating any storage, collection or operation on personal data, within the constrains of the agreed upon purposes.
- Tactics:
- **Distribute**: partitioning personal data so that more access is required to process it.
- **Isolate**: processing parts of personal data independently without access or correlation to related parts.

Abstract

- **Abstract**: limiting detail as much as possible by summarizing or grouping any storage, collection or operation on personal data, within the constraints of the agreed upon purposes.
- Tactics:
- **Summarize**: extracting commonalities in personal data by finding and processing correlations instead of the data itself
- **Group**: inducing less detail from personal data prior to processing, by allocating into common categories.

Inform

- **Inform**: providing as abundant clarity as possible for supplyig, explaining and notifying on storage, collection, retention, sharing, changes, breaches or operation on personal data, in a timely manner, within the constraints of the agreed upon purposes.
- Tactics:
- **Supply**: making available extensive resources on the processing of personal data, including policies, processes and potential risks.
- **Notify**: alerting data subjects to any new information about processing of their personal data in a timely manner.
- **Explain**: detailing information on personal data processing in a concise and understandable form.

Control

- **Control**: providing as abundant means as possible for consenting to, choosing, updating, and retracting from storage, collection, retention, sharing or operation on personal data, in a timely manner, within the constraints of the agreed upon purposes.
- Tactics:
- **Consent**: only processing the personal data for which explicit freely-given and informed consent is received.
- **Choose**: allowing for the selection or exclusion of personal data, partly or wholly from any processing
- **Update**: providing data subjects with the means to keep their personal data accurate and up to date.
- **Retract**: honoring the data subject's right to the complete removal of any personal data in a timely fashion.

Enforce

- **Enforce**: ensuring as abundant commitment as possible for creating, maintaining and upholding policies and technical controls regarding storage, collection, retention, sharing, changes, breaches or operation on personal data in a timely manner within the constraints of agreed upon purposes.
- Tactics:
- **Create**: acknowledging the value of privacy and deciding upon policies which enable it, and processes which respect personal data.
- **Maintain**: considering privacy when designing or modifying features, and updating policies and processes to better protect personal data.
- **Uphold**: ensuring that policies are adhered to by treating personal data as an asset and privacy as a goal to incentivize as a critical feature

Demonstrate

- **Demonstrate**: ensuring as abundant evidence as possible for testing, auditing, logging, and reporting on policies and technical controls regarding storage, collection, retention, sharing, changes, breaches or operation on personal data in a timely manner within the constraints of the agreed upon purposes.
- Tactics:
- **Log**: tracking all processing of data without revealing personal data, securing and reviewing the information gathered for any risks.
- **Audit**: examining all day to day activities for any risks to personal data and responding to any discrepancies seriously.
- **Report**: analyzing collected information on tests, audits, and logs periodically to review improvements to the protection of personal data.