
CERN

Stress Free Data Privacy Protection

David Foster
CERN Data Privacy Protection Officer
More information: odpp.web.cern.ch
July 2017

#3 Privacy By Design

In 10 minutes or less ….

Purpose and outcomes

- After going through this presentation you should be able to appreciate:
  - Appropriate considerations when designing or implementing new services
  - What is meant by Privacy by Design
  - What is meant by Privacy by Default

Prerequisites

- #1 The Basics

Core principles of privacy by design

- Be user centric
- Be proactive
- Make privacy a design requirement
- Design a no-compromise approach
- Design end-end security
- Be transparent
- Implement privacy by default

Be user centric

- Protecting the rights of the individual is core to the design.
- The fundamental premise is that personal data belongs to the individual concerned.
- Functionality cannot take precedence over protecting privacy rights.

Be proactive

- A proactive mindset.
- It is better to prevent anticipated problems rather than “clean up” afterwards
  - e.g It is better to block access to restricted material rather than continuously monitor looking for infringements.
- Consider the risks of accidental or over-processing of personal data in the service design.

Make privacy a design requirement

- In general, adding privacy “after the fact” is as difficult as adding computer security or quality considerations.
  - Once processing has been done, it cannot be undone.
- Reduce the amount of personal data
  - Minimise the data collected.
  - Anonymise or pseudonymise wherever possible.

Design a no-compromise approach

- There are rights associated with the processing of personal data.
  - Consider how to implement the right to access the data being held and processed.
- Systems that collect, access or process personal data cannot compromise on the fairness (and legality) of processing.
  - “I just kept these files that contain personal data because they have other data too that I might need”

Design end-end security

- This applies to the processing of personal data at all stages of the lifecycle.
  - Collection
  - Transfer
  - Storage
  - Processing
  - Destruction
- Implement appropriate technical measures such as encryption.
- Protection throughout the lifecycle applies to physical files as well as electronic formats.

Be transparent

- Processing of personal data is done for one of a number of legitimate reasons, the most common being:
  - To fulfil a contractual relationship (e.g. employment)
  - For the legitimate interests of the organisation.
  - With the consent of the individual
- The handling of the personal data by the service must be detailed in a privacy notice (See video #002 in this series)
- The design and implementation of the service should demonstrably show how the processing conforms to the privacy notice.

Implement privacy by default

- The trend is towards reducing the processing of personal information wherever possible.
  - “opt-out” check boxes are deprecated.
  - Browser settings can indicate consent but only where the default was to disallow processing.
- Systems must be designed so the individual is made clearly aware of the processing taking place.
- Informing the individual of processing or the consequences of their positive actions must be done at the point of collection or processing.

From here to there

- Many services receive data from other services.
  - This is processing.
- Many services pass on data to other services.
  - This is processing.
- Be clear what personal data you may be handling and make sure the processing is both justified and transparent to the individual.
- Services are accountable for the processing they do.
  - It should be possible to independently verify the handling of personal data by the service.

For more information

- You can give feedback by mailing privacy.protection@cern.ch
- You can consult the Office of Data Privacy Protection website: odpp.web.cern.ch
- You can pose questions or report incidents directly to the odpp service through Service Now.


DONT
PANIC