Data Protection @ CERN IT

Andrei Dumitru
CERN IT Department
10th of October 2018

Disclaimer

The recommendations outlined here are currently used in the CERN IT department services and they may change over time as the common Data Protection best practices evolve.

General Data Protection Regulation

Is a regulation in EU law on data protection and privacy.

Applies to the processing of personal data of data subjects who are in the Union.

Entered into force on the 25th of May 2018.

What is personal data?

From the CERN Office of Data Privacy Protection (ODPP)

> "Personal Data" or "Personally Identifiable Information" (PII) consists of any data related to an identified or identifiable individual - a "Data Subject". An identifiable individual is someone who can be identifiable from that data and other information or identifiable by means reasonably likely to be used related to that data.

Is an IP address personal data ?

Short answer: YES!

It is prudent to consider any unique identifier as personal data.

Check the ODPP website for the complete explanation.

CERN and GDPR

CERN is an International Organization (IO)

- IOs are mentioned explicitly in the GDPR
- "International Organisation" means an organisation and its subordinate bodies governed by public international law
- similar to a *third country* ("third countries or international organisations")

CERN collaborates with entities that are subjected directly to GDPR

- needs to ensure an adequate level of protection

Data Protection @ CERN

CERN is goverened by Operational circulars

- Operational Circular 11 (in review) will cover **Data Protection at CERN**

CERN Office of Data Privacy Protection

- the competence center for the best practices on data protection at CERN

Privacy Notices

What is a Privacy Notice ?

- the way we explain to the users of our services what will happen to their personal data
- easy-to-read notice in *"a concise, transparent, intelligible and easily accessible form, using clear and plain language"*

Examples:

Computer Security Service

Site Security Service

CERN Alumni

Structure of a Privacy Notice

Data used by the service / Personal Data we process

- personal data the service processes, the purpose, the legal basis and the source
- processing means any operation, automated or not, which is performed on personal data

Data stored by the service / Personal Data we keep

- personal data the service stores, for how long and why

Who at CERN has access

- what personal data is visible, sent, stored, exposed, accessible, by which services/teams at CERN and for what purpose

Transfer Data externally / Personal Data we may transfer to others

- what personal data is shared outside CERN, with whom and for what purpose

Data Protection in the IT Department

Privacy Notices in ServiceNow for services offered by CERN/IT

- exist for all IT services
- only visible internally for now
- review and update ongoing taking into account the IT Data Protection Working group recommendations and guidelines

IT Data Protection Working Group

One member from each team (group) in the IT department

Goals:

- study the existing data protection Privacy Notices
- advise on a recommended set of best practices for CERN IT

IT Data Protection Working Group

Created a guideline on what the Privacy Notices should contain in each section so they will be uniform across the department.

Defined common terminology/naming conventions that should be used across all PNs

- for Personally Identifiable Information(PII), naming conventions are based on the most common terms and synonyms used in the existing PNs

Proposed data retention periods for Personally Identifiable Information

- based on the purpose of the data retention (what is the data used for)

Presentations on Data Protection for each team.

Data Retention Periods

Purpose (data used for)	Recommended maximum retention period
Service Troubleshooting and Support	3 months
Computer Security Incident Response	1 year
Authentication and Authorization	Until the resource is deleted.

Data Retention Periods

Purpose (data used for)	Recommended maximum retention period
Resource ownership	For the lifetime of the resource.
Audit	Depends on the requirements and needs a justification.
Analytics / Statistics	Use only anonymized data.

Next steps

1. Final review of Privacy Notices following the publication of OC11

2. Analyze the use-cases that may not (initially) fit in the proposed data retention recommendations.

3. Publish the Privacy Notices

4. Long term - update services if required

home.cern