Implication of Data Privacy Implementation at CERN

EP-SFT Group
(Inform, Impact, Implementation)

Barbara Brugger for EP & RCS Data Privacy Implementation Project
April 15th 2019

I am here to help during this journey! 😊
Introduction

The General Data Protection Regulation (GDPR) which is a European regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, entered into force in May 2018.

CERN, by virtue of its status of intergovernmental organisation governed by public international law, is not subject to the law of other intergovernmental organisations. As the GDPR is part of the internal law of the EU, another intergovernmental organisation, it is not directly applicable to CERN. Therefore, CERN cannot and will not apply for an adequacy decision from the European Commission. Nevertheless, CERN takes data protection seriously and strives to stay up-to-date with the evolutions of society.

• What is the main internal rule applying at CERN

In light of the recent developments in data protection matters, CERN saw the GDPR as a catalyst to update its internal rules on the processing of personal data (Operational Circular n°11 – OC11).

Such rules are inspired by best practices and the general principles that can also be found in the GDPR. Among others, OC11 provides for the legal tools for transferring personal data to and from external entities, be they subject to the GDPR or not.

Note that I will refer to «OC11» throughout this presentation!
OC11 in a nutshell

- **Purpose of this Operational Circular n°11**
  - Set out the Organisation’s approach to data privacy protection, as well as the associated rights and obligations

- **Status**
  - Entered into force in January 2019. **Full implementation** of the circular will be subject to an **implementation calendar*** approved by the Director-General
  - **Legal obligation** to answer persons’ requests in **January 2020**, **BUT persons can already exercise their rights** and we should **make our best** to answer them

- **Who is concerned**
  - All persons whose Personal Data is processed by CERN, and
  - All persons or entities processing Personal Data on its behalf

What is considered as **personal data**

Any information, in any form or medium, relating to an identified or identifiable person ("Data Subject"*)

**Examples**

- Biographical information or current living situation [e.g. names, date/place of birth, family situation] and information about education, salary, tax information
- Car plate numbers, personal financial details, photos
- Workplace data [e.g. IP/MAC Address, logs, computing accounts]

* Data Subject, is any person whose Personal Data is processed by CERN. For the purpose of OC11, it also includes any person authorised to act on behalf of the Data Subject concerned.
What is considered as **sensitive personal data**

Sensitive personal data is a specific set of "special categories"

These categories are:

- Physical or mental health
- Genetic or biometric data [e.g. Retinal scan for the LHC]
- Racial or ethnic origin [e.g. Food preference Halal, Kosher]
- Sexual orientation [e.g. Member of the LGBT E-group]
- Political, religious or philosophical opinions or beliefs

➢ General prohibition
What is processing (sensitive) personal data

Collection + Exploitation + Destruction

- **All activities** relating to personal data, from:
  - its initial **collection** & its **use**,
  - its **retention** & its **storage**,
  - its **access** & its **display**,
  - its **duplication** & its **transfer**, and
  - its **destruction**.

- **Examples**
  - Collecting and/or transferring CV;
  - Accessing and/or displaying DB containing personal data;
  - Posting someone’s photo on a website.
What are the **requirements for processing**

- A lawful basis exists
- Data processing principles are respected
The Six Data Processing Principles

Good faith: Respect of person’s rights

- Access, retention, IT tools’ security, Security of paper
- Proportional to the stated purpose
- Time limitation
- Correctness: Always verify!

Information/transparency through Records of Processing Operations that detail the Personal Data Processing carried out by a service
Six Legal bases for personal data processing

Freely given, specific, informed and unambiguous person’s consent

To allow for an efficient functioning of CERN provided it does not outweigh the privacy of the data subject

Necessary for the purposes of maintaining CERN’s archives, for scientific or historical research, or for the preparation of statistics

Lawfulness of processing

Consent of the data subject

Contract with the individual exists

Legitimate interest

Consent of the data subject

Public interest

Legal obligations

Vital interest

For the performance of a contract with the person of concern

To apply or comply with internal or external rules and regulations

It is vital that specific data are processed for matters of life or death

Principle: No processing unless it is based on one of these bases
Person’s Rights & How to exercise them

Right:
• to information
• to access
• to object and to correction
• to request temporary suspension of processing
• to deletion
• to portability
• in respect to automated decision-making

• Request through common interface
• Right to a written response
• CERN has the discretion to deny request, if it deems it for example unreasonable, abusive, obstructive to the purpose of processing or if granting the request would involve a disproportionate effort
Preliminary considerations

• Information and Agreement
  ➢ Ensure Data Subject is informed & you received his/her freely given consent

• Minimum and essential information processed for a stated time
  ➢ Do not archive for ever (sensitive) personal data “just in case” you may need them

• Well defined and streamlined processes
  ➢ Use as much as much as possible central databases to consult personal data [e.g. Foundation] and if you send personal data by emails [e.g. CV, Letters of Intent] ensure the data processing principles are respected

• Ensure that only the right people have access to the right information
  ➢ Ensure your e-groups are up-to-date [e.g. for static e-groups remember to manually remove any person leaving the group or CERN in order to restrict access]
OC11 Implementation

• Data Privacy Coordination Committee *Chaired by J. Purvis*

- Aiming for **CERN common approach:**
  - implementation of the rights and obligations conform to OC11
  - ensure that personal data are handled in an appropriate and harmonised manner across CERN

- Requirements:
  - common “retention periods” (DPA guidelines) -> How long to keep personal data
  - review of organisational processes -> How do we handle it so far
  - data handling and records keeping processes -> What we keep and how we transfer it

• Data Privacy Adviser *Gabriele Thiede*

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

• Departmental Data Privacy Protection Coordinator *Myself*

  - Coordinating the OC11 implementation within EP and RCS
A Service (OC11 context) : One or more activities involving the processing of personal data on a regular basis for the benefit of CERN [e.g. Computing Teams]

Service Catalogue: Single interface where all services processing personal data (among other services) are listed

Records of Processing Operations detail the Personal Data Processing carried out by a service

---

**Milestones**

- **GDPR entered into force**: 25 May 2018
- **OC11 Approved by CCP**: 18 October 2018
- **Service Catalogue: Structure complete**: 12 November 2018
- **ONC11 entered into force**: January 2019
- **Draft Records of Processing operations ready**: 31 March 2019
- **Records of Processing Operations comply with OC11**: 30 June 2019
- **Records of Processing Operations comply with OC11**: January 2020
Training provided at CERN on this matter

- **E-learning awareness training**
  - https://espace.cern.ch/support-e-learning/privacy/_layouts/15/start.aspx#/SitePages/Module%201.aspx

- **Free of charge in-class training sessions** for everyone processing personal data on a regular basis
  - Respecting Privacy in the processing of personal data at CERN
Summary

• OC11 is applicable to any person working at or on behalf of CERN, and any other person whose personal data is processed by CERN
  ➢ Everyone shall feel concerned

• Legal obligation to answer Data Subjects’ requests as from January 2020
  BUT data subjects can already exercise their rights
  ➢ Make our best to answer their request

• Services processing personal data on a regular basis must:
  • be registered in the Service catalogue, and
  • keep records of its processing activities for transparency
  ➢ If you are processing personal data on a regular basis, contact me!

• I remain at your disposal if you have questions on this matter

THANK YOU! 😊
BACKUP / DETAILS
Concrete examples

• Copy of ID card or bank account details: Can I keep it for ever “just in case”?
  ➢ No, delete the scanned copy once the purpose for collecting is fulfilled
    [e.g. in DFS, on your Desktop, in Email received/sent/«Deleted items» boxes, printed copy, clear your Cache]

• Food preferences: Can I still ask?
  ➢ Yes, BUT, Do NOT keep such information as there might be some “Sensitive Data” hidden
    [e.g. Kosher, Halal]

• Photos during a social event: Can I continue processing them?
  ➢ Yes, BUT as long as data processing principles are respected