

# The Processing of Personal Data at CERN (OC 11)

## EP R&D Website

*Barbara Brugger for EP & RCS Data Privacy Implementation Project*

March 5<sup>th</sup> 2020



# Reminder

- **May 2018: General Data Protection Regulation (EU regulation)**
  - **Not directly applicable to CERN** by virtue of its status of intergovernmental organisation governed by public international law
- **January 2019: OC 11\* entered into force**
  - *Purpose:* to set out CERN's approach to data privacy protection
  - *Applies:* to all persons whose personal data is processed by CERN and all persons or entities processing personal data on its behalf
- **January 2020: Processing operations of personal data**
  - Shall comply with OC 11

# What is considered as (sensitive) personal data



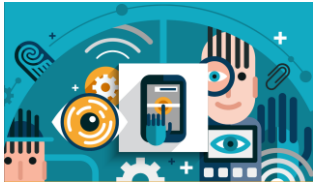
Any information, in any form or medium, relating to an **identified or identifiable person**

## Examples

Biographical information or current living situation [e.g. names, date/place of birth, family situation, **education**]

Car plate numbers, personal financial details, **photos**

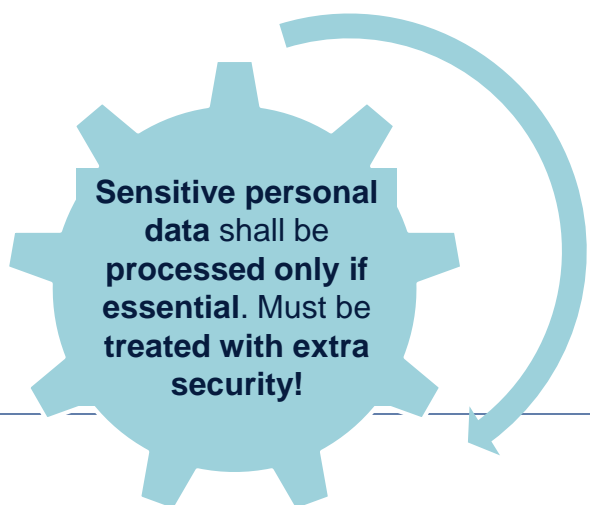
Workplace data [e.g. **IP Address**, logs, computing accounts]



**Sensitive personal data** is a specific set of “special categories”

These special categories of **sensitive personal** data are:

- Physical or mental health
- Genetic or biometric data
- Racial or ethnic origin
- Sexual orientation
- Political, religious or philosophical opinions or beliefs



**Sensitive personal data** shall be processed only if essential. Must be treated with extra security!

# 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 in your context**
  - Displaying a “résumé” of someone that may include the date of birth;
  - Posting someone’s photo on a website;
  - Providing a link to a personal page [e.g. “Linkedin” link].

The **Processing** of Personal data **shall always** respect the **Six Data Processing Principles\*** and **Six Legal bases** for processing\*

[e.g. data collected only with a legitimate purpose, proportional to the stated purpose, kept as long as necessary, based on the consent or contract]

# 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**

- The official channel to exercise these rights is via a [web form](#) that will be then managed by the [Office of Data Privacy Protection](#)
- ✓ Ensure you have a mechanism that allows people exercising their right [e.g. link to the official web form, a generic email address or through the "Contact" form]

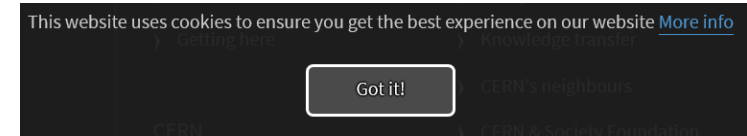


\* Data Subject is entitled with some conditions to receive his/her data in a reasonable and reusable format. See § 77-78 of OC 11 for further details

# Practical Elements to think about at this stage

## Information and Transparency are key elements!

- Do you plan to provide a “disclaimer” regarding the **contents**? If yes:
  - Proposal: «*The contents found in the web pages are for information purposes only*» “ATTRACT” [Legal notice](#)
- Will you use **cookies**? If yes:
  - Inform people and give the possibility to manage them
- **Email addresses**: Do you intent to store and use them? Who has access to this data? Depending on the answer you may think about adding in the “Contact” page, either:
  - “*Your email address will only be used by administrators of the website (correct?) to answer your requests and enquiries, and we will treat the data confidentially. We will keep your e-mail address data for/until XXX and will not transfer it*”, or
  - “*By ticking this box, I acknowledge and consent that the EP R&D administrators of this website (correct?) will use the email address provided in this contact form only to answer my requests or enquiries. I understand that I can withdraw this consent at any time without reason by sending a communication to that effect to [XXX@cern.ch](mailto:XXX@cern.ch)*”
  - Limit the number of persons having access to this data



# Practical Elements to think about at this stage

- Will you keep **personal data** including the photos **of former members**? If yes, you should:
    - **Think of keeping** only the **names** -> **Sensitive data** can be **hidden in personal pages**
    - **Obtain and Keep** the **record of the** freely given **consent** from former members
    - **Define a retention period** and put in place a **mechanism to destroy** the **data** in due time
    - **Define a purpose** for this processing, and who will have access to this data
  - **Ensure** that only the **right people** have **access to** the **right information**
    - **Can everybody subscribe to your E-groups?**
      - ✓ Ensure security access to E-groups and to Work Packages as Photos and Résumé are displayed
    - **Can someone change someone else's profile?** If yes,
      - ✓ Ask yourself if is it legitimate? If not,
      - ✓ Put in place technical security
    - **Keep e-groups' membership up-to-date** (especially for former members)
      - ✓ "Correctness of data" is one of the Six Data Processing Principles
- **Mitigating the risk of data breach**

# Training provided at CERN

- **E-learning awareness training**
  - **Mandatory** for everybody
    - ✓ Respecting Privacy in the processing of personal data at CERN – e-learning
- **Free of charge in-class training sessions**
  - **Mandatory** for everyone processing personal data on a regular basis and Service Owners\*
    - ✓ 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**
- ❖ The **implementation shall**
  - **Respect the Six Data Processing Principles**
- ❖ **Processing operations of personal data shall**
  - **Comply with OC11 as from January 2020**
- ❖ **Training is available at CERN Free of charge**

**THANK YOU!**



# BACKUP / DETAILS

# What are the **requirements** for processing



# The Six Data Processing Principles

**Good faith:** Respect of person's rights

Access, retention,  
IT tools' security,  
**Security** of paper

**Time** limitation



**Proportional** to the stated purpose

Correctness:  
**Always verify!**

Information/**transparency**

# 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



For the performance of a **contract** with the person of concern

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

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**

# Good reflexes to have as a Service

|                                |  |   |
|--------------------------------|--|---|
| REFLEX<br>1<br>RELEVANCE       | <b>COLLECT ONLY ESSENTIAL PERSONAL DATA</b><br>Ask yourself: What is my objective? Which data are mandatory to reach this objective?<br>Do I have the right to collect these data? Is it accurate?<br>Are the Data Subject concerned ok with that? | ➔ Data of former Members: One could think on keeping only the names   |
| REFLEX<br>2<br>TRANSPARENCY    | <b>BE TRANSPARENT</b><br>A clear and complete information is the foundation of a trusted contract that binds you with the people whose data you are processing.  | ➔ Using cookies? then announce it   |
| REFLEX<br>3<br>RIGHTS' RESPECT | <b>THINK ABOUT PEOPLE'S RIGHTS</b><br>You must respond as soon as possible to requests for consultation, rectification or deletion of data.  | ➔ Allow data subject exercise their rights:<br>➔ Mechanism such as generic email address or a link to your "Contact" form |
| REFLEX<br>4<br>CONTROL         | <b>KEEP CONTROL OF DATA</b><br>The sharing and circulation of personal data must be supervised and contracted to protect them at all times.  | ➔ Ensure E-groups & Work packages accessible by right persons and membership updated                                      |
| REFLEX<br>5<br>RISK MGT        | <b>IDENTIFY THE RISKS</b><br>You process a lot of data, or sensitive data or have activities with special consequences for people, specific measures may apply.  | ➔ Sensitive data can be hidden in personal pages e.g. Greenpeace active member  |
| REFLEX<br>6<br>SECURITY        | <b>SECURE YOUR DATA</b><br>The security measures, computer as well as physical, must be adapted according to the sensitivity of the data, and the risks which weigh on the people in the event of an incident.                                     | ➔ Ensure that someone cannot modify someone else's profile or Work packages   |

# Declare a Service in the CERN Service Portal

- **“Service” concept: Definition of a service (OC11 context)**

A **Service** in the sense of the OC 11 is a grouping of activities involving the processing of Personal Data on a regular basis for the benefit of CERN. This Service does not correspond necessarily to an organic unit or a functional area.

The OC11 distinguishes two types of services:

Y  
O  
U  
R  
C  
A  
S  
E

- **Controlling Services**

- Determine the purpose** (Why?) **and the means** (What? How? For how long?) for their processing of personal data
- Responsible for **implementing appropriate technical and organisational measures** to demonstrate that its processing activities are compliant with the OC11

Need to:

- ❖ Be registered in the Service Catalogue, and
- ❖ Establish Records of Processing Operations

- **Processing Services**

- Process** personal data solely **on behalf of controlling services**
- Responsible for **processing activities in accordance with the controlling service's instructions**

NO need to:

- ❖ Establish Records of Processing Operations

BUT need to:

- ❖ Be registered in the Service Catalogue

- In both cases, a single **Service Owner** needs **to be nominated**

# Service Owner

A Service has an **owner**; this person is accountable for the processing of the Personal Data by his/her Service. This means that the person takes responsibility for the activities carried out by the Service. Service Owners shall be member of the personnel of CERN.

A **Service shall have a single owner**, multiple owners are not allowed.

- Definition, Role and Obligations:

- *Definition:* “A Service Owner is the person accountable for the processing of Personal Data by his/her Service” (article 14 of the OC11)
- *Role:* Service Owners’ role as described in the article 26 of the OC11: “Each Service Owner shall be responsible for his or her Service’s compliance with this Circular.”
- *Obligations:* Service Owners have in particular to make sure that their Services
  - a) observe the general principles set out in chapter IV of the OC11, and
  - b) execute the duties and responsibilities as detailed in chapter VI, for example:
    - ❖ The establishment of Records of Processing Operations (chapter VI.A)
    - ❖ The correction and deletion of personal data (chapter VI.B)
    - ❖ The establishment of data retention periods (chapter VI.C)
    - ❖ The execution of Data Privacy Impact Assessments (chapter VI.E) mostly in case of sensitive data processing

- Responsibility:

- The responsibility is internal to CERN and is therefore regulated by the part of Chapter VI of the Staff Rules and Regulations on discipline.
- The Service Owner is therefore subject to CERN’s administrative and disciplinary procedures for his/her actions and omissions regarding the obligation laid down in art. 26 of the OC11.
- Ultimately, the Service Owner is responsible towards the Director General who is the legal representative for the Organization towards “the outside world”. CERN is the Data Controller as mentioned in article 8 of the OC11.