Data Protection and Records Management at EMBL

45th Meeting ICA / SIO, NATO Headquarters, Brussels, Belgium
20-22 May 2019

Marie Caillot
Records and Information Manager,
Administrative Director’s Office

EMBL
1. Data Protection at EMBL: Why Have a Specific Framework?

2. A Few Words About Records Management at EMBL

3. Data Protection and Records Management
EMBL’s specific status and its impact on Data Protection

An international organisation...
- Established by Treaty with 26 State Members in 1974
- Privileges and Immunities
  - inviolability: premises, files (staff and representatives's official files and documents), and archives
  - Exemption of national jurisdictions
  - Exemption of applicability of national laws

... and a scientific institution
- Promoting cooperation among European States in fundamental research
- Data transfer: a key component for scientific work
- As a scientific organisation, EMBL processes:
  - Human biological materials (e.g. genetic data and data concerning health: blood, tissues, biopsies, cells, etc.) as well as the analysis of data derived from these materials
  - But also personal data of:
    - External scientists (visitors using EMBL scientific facilities, attendees of workshops, courses and conferences)
    - ... besides other personal data usually processed within the organisation
Consequence:

Exemption from GDPR:

→ Although physically located in Europe, having strong ties with European scientific community (data transfers) and receiving EU fundings, EMBL does not belong to the EU system

→ Specificity of scientific and organisation activities engaged EMBL to define its own data protection framework,
  → to reach a level of data protection inspired by GDPR...
  → ... while respecting EMBL’s privileges and immunities
Why have EMBL’s Own Data Protection Framework (IP68)?

- Data protection is a fundamental human right
- Safeguards are needed for:
  - **ensuring EMBL’s scientific collaboration worldwide**
    - GDPR, Chap. 5: EU insiders are allowed to transfer personal data to third countries or international organisations who can demonstrate that safeguards are in place
    - demonstrate compliance with data protection principles to external scientific collaborators
    - ensuring EMBL stakeholders (incl. funders) that we comply with data protection principles
  
  - **ensuring data subjects’ rights**
    - EMBL framework aims at preventing risks e.g.:
      - Fairness and legitimate purpose (e.g. during staff recruitment)
      - Identity theft or fraud (e.g. hacker steals credit card data)
      - Financial loss (e.g. allowance denied due to outdated HR record)
      - Damage to reputation
      - Data breach (e.g. medical data)
      - Unauthorised reversal of pseudonymisation (e.g. genetic data)

  - … while maintaining EMBL privileges and immunities
EMBL’s Data Management Internal Framework

Internal Policies

- IP53 – Use of Human Biological Material (2013)
- IP54 – acceptable computer and network facility use (rev. 2013)
- IP68 – General Data Protection (2018)

Internal Rules and Regulations

- Finance regulations and internal rules (last rev. 2017)
- Staff rules and regulations (last rev. 2017)
- Archives’ Statement (last rev. 2018)
- Records Management Framework Policy (last rev. 2018)
- Archives Categorisation Guideline (2019)

Documents, Tools and Guidelines

- Data Privacy notices
- Records of processing activities
- Filing structure guidelines
- retention schedules
- Etc.

More specific frameworks

- Staff rules and regulations (last rev. 2017)
- Archives’ Statement (last rev. 2018)
- Records Management Framework Policy (last rev. 2018)
- Archives Categorisation Guideline (2019)
Data Protection: project’s timeline and governance

• 2016: Task force (IT, Legal Services) on Data Protection
• June 2017: a DP. project officer is recruited, project launched
• Autumn 2017: project plan is endorsed by Steering Committee
• January 2018: draft of Internal Policy no. 68 on Data Protection is discussed within Working Group

⇒ **Steering Committee**: Administrative Director (project owner), 2 high level scientists, Heads of IT (HD/EBI), Deputy Head of Legal services
⇒ **Working Group**: IT engineers (2), Records Manager (1), HR Manager (1), Grants Officer (1), System Engineer (Finance) (1), Courses and Conferences Managers (2).

• May 2018: Data Protection Internal Policy (IP no. 68) is approved by Director General and official statement made available on EMBL website ([link](#))

• From June 2018:
⇒ Steering Committee started setting-up of a supervisory authority: **Data Protection Committee**
⇒ **Data Protection Officer** is appointed (independent function)
⇒ **Data Protection Coordinator** (under Administrative Director)
⇒ DPO and DP. Coordinator started advising controllers on formalising/optimising critical personal data processing activities
1. Data Protection at EMBL: Why Have a Specific Framework?

2. A Few Words About Records Management at EMBL

3. Data Protection and Records Management
Creating the Records Management Function at EMBL (1/2)

• A new function (2016)
• Developing and overseeing the implementation of a records management plan for the organisation's administration

Project’s scope:
- Under the Administrative Director’s direct supervision
- EMBL Administration (14 units, 6 sites located on 5 countries: Germany, France, Italie, UK and Spain)
- Initial focus: Heidelberg (from 2017), the 5 other Sites from 2018 onwards
- Establishing rules and procedures for managing authentic and reliable records over their lifecycle (P/E)
- Digital RM: accompanying change from current existing EDMS to EDRMS (P/E)
- Approach: project management

• References: international standards, DIRKS methodology, benchmark with other international organisations... adapted to EMBL’s context
Creating the Records Management Function at EMBL (2/2)

Establishing:

- Working Group
- RM strategy
  - Framework Policy
  - Project Implementation Plan
- RM Project
  - 6 Work Packages
  - Defining and implementing: procedures, guidelines, systems to ensure administration’s records management
- Review step
  - Development
  - Improving and developing the RM plan

PRE-IMPLEMENTATION PHASE

2016 (Sem. 2)

2017 (Sem. 1)

IMPLEMENTATION PHASE

From 2017 (Sem. 2)

2022
1. Data Protection at EMBL: Why Have a Specific Framework?

2. A Few Words About Records Management at EMBL

3. Data Protection and Records Management
Personal Data and Administrative Records

- In an administration’s records, personal data are numerous: they are processed as part of almost all administrative processes

- In 2017-2018, retention schedules project: approx. **400 main records types and associated processes** were identified, approx. **250 of them** relate to personal data

- Personal data are more and more collected and stored on electronic mediums, which raises specific constraints

- Staff’s personal data: under EMBL’s framework (IP no. 68) but EMBL also handles data from EU individuals (visitors, applicants to jobs)
  - Critical to demonstrate EMBL commitment to comply to data protection principles
Personal Data Principles and Records Management

IP 68 substantive provisions

- Clear definition of roles on data processing
- Notion of data quality:
  - storage limitation
  - Legal basis (consent or other)
- Transparency
- Purpose limitation
- Data minimisation
- Accountability
- Accuracy
- Integrity and confidentiality

Records Management

- RM Framework Policy defining data stakeholders’ roles
- **Data retention**: defining our own framework of retention policies, taking into account EMBL 5 host countries’ requirements + IP68 + our grant funders’ requirements
- **Transparency**: a key objective of records management is to ensure sustainable and transparent processes: in the way data is processed, but also on the functioning of an organisation
- Accountability
- Accuracy
- Integrity and confidentiality

ISO 15489:2016
Impact on Records Management: initiatives

Collaboration with DPO and DP. Coordinator

• Cross-contributions in Data Protection’s and Records Management’s Working Groups

• Role of DPO and DP. Coordinator in the retention schedules’ project (2017-2018): assessing retention rules from personal data’s perspective as well and ensuring that the rules of destruction are compliant to data protection’s principles

• IP68: notion of recordkeeping (transparency, accuracy and accountability):
  → Record of Personal Data Processing Activities: identification of types of records; description of activities; information for data subjects; retention periods (also specified in Data Privacy Notices)
  → partially covered as part of retention schedules’ project

• Data Categorisation Guideline (2019) (RM, IT) (accountability, transparency, confidentiality): defining levels of sensitivity for each data type received or produced at EMBL, with impact on storage and security measures, pre-defined metadata according to level of sensitivity

• EDRMS project (RM, HR, IT) (storage and data minimisation, transparency, accuracy, accountability, integrity and confidentiality): ensuring that features enabling Data Protection are represented
Conclusion

Data Protection and Records Management: two complementary fields

• GDPR provided a momentum for data management in general
• Convergence of concepts
• Compelling force of data protection, which can be useful to enforce records management’s initiatives, e.g.:
  → identification of personal data and processes
  → positive impact on the retention schedules project
  → enhanced security: impulse of Data Categorisation Guideline and redefined of access rights for our information systems
Thank you for your attention

Marie Caillot
Records and Information Manager, Administrative Director’s Office
marie.caillot@embl.de