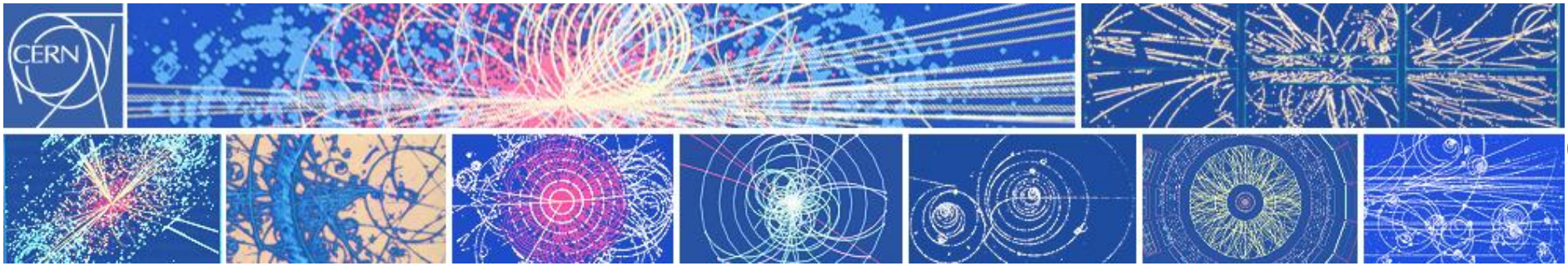

Data Protection in Intergovernmental Organizations

Workshop
7 February 2013

K. Ernst
S. Lüders
C. Viala

Data Protection Frameworks

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

  http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

  http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF

- National data protection laws, e.g. the Swiss Federal Act on Data Protection

  http://www.admin.ch/ch/e/rs/2/235.1.en.pdf

Common Personal Data Protection Principles

Personal data must be:

- processed fairly and lawfully;
- collected for a limited purpose and not kept longer than necessary;
- adequate, relevant and not excessive in relation to the purpose for which data is collected and processed;
- accurate, and where necessary, kept up to date;
- collected and processed pursuant to the rights of the person concerned;
- stored and processed securely;
- not transferred without adequate protection;
- treated confidentially.

Data Protection Initiative at CERN

An ad-hoc Working Group (composed of IT security and legal staff) identified a need for:

1. classification and improved protection of personal data of CERN Contributors (i.e. all persons working at or on behalf of CERN), taking into account the growing digitalization of data.

   → the protection of personal data of CERN personnel is a legal obligation under CERN‘s Staff Rules and Regulations.

2. consistent and comprehensive regulations on the use and flow of data within CERN to ensure a secure, qualitative and effective handling of the Organization‘s activities and related data.

   → the protection of other CERN data is not a legal obligation but a homogenization of existing rules is desired, considering the amount of data generated by CERN in different areas (science, administration, CERN governing bodies)

Data Protection Issues Encountered (1)

1. Which data does CERN hold?

2. What is CERN data? Which is internal data, which is external data (difference between ownership and possession)?

3. What data should be covered by the CERN data protection policy?

4. In terms of protection, should one distinguish between personal and other data?

Data Protection Issues Encountered (2)

5. Data classification: which categories, how many, for which type of data? Whose responsibility is it to classify data?

6. Data access and sharing: who can access different types of data? Who can grant access to data to whom? What is the role of CERN‘s IT department in this area?

Data Protection Issues Encountered (3)

7. Data storage: which type of storage for digital and hardcopy data? Whose responsibility? How to handle (inter-)dependencies of data storages?

8. Data retention: which retention periods for which type of data? Digitalization of all data (IT issues)? Whose responsibility?

9. Data destruction: how to destroy data (difference between digital and paper data)?

Food for Discussion

1. What is your IGO‘s approach to (personal) data protection?

2. To which extent should IGOs comply with the principles of national/international data protection schemes?

3. What does your IGO cover by its data protection scheme, or, in case it does not have such a scheme, what do you think should be covered?