EUROPE BIOBANK WEEK

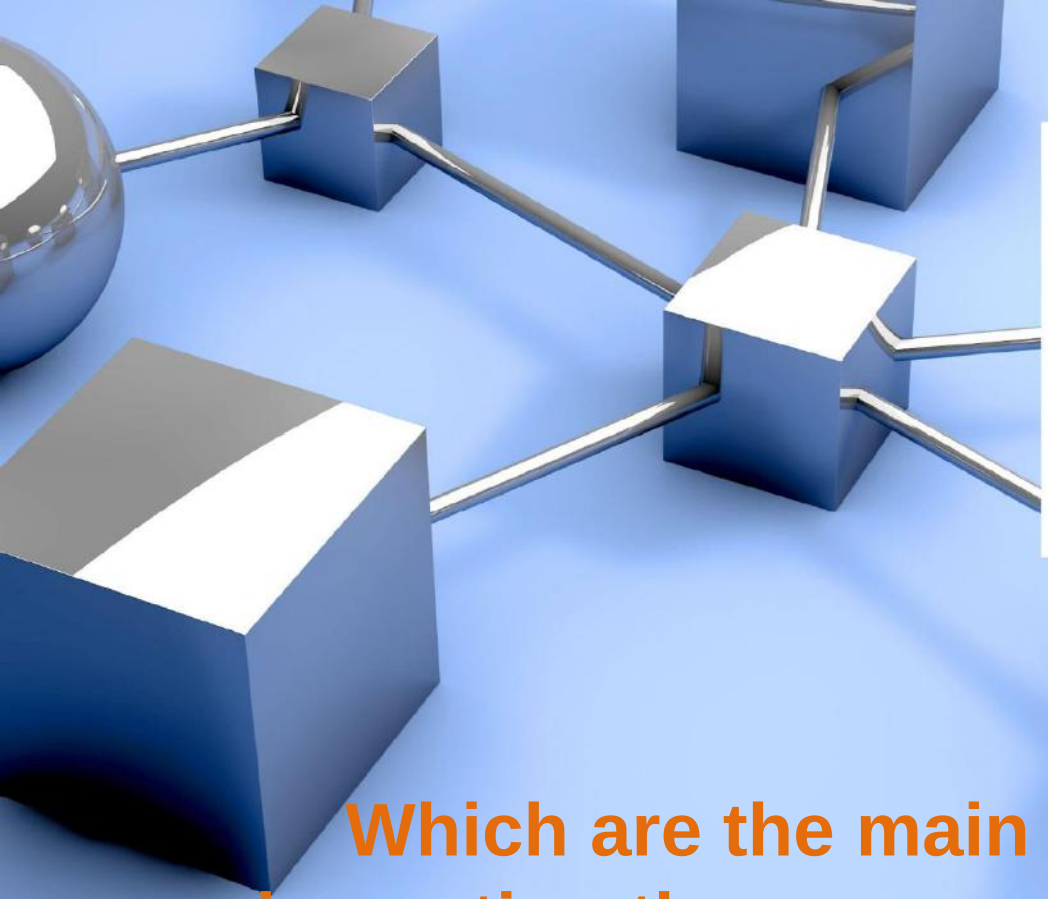
SEPTEMBER 13-16, 2016
VIENNA - AUSTRIA

Gauthier Chassang: "What are the main new requirements impacting the governance of data processing in research biobanking under the EU General Data Protection Regulation?"

BBMRI-ERIC® gateway for health

BBMRI.at Biobanking and BioMolecular resources Research Infrastructure Austria

European, Middle Eastern & African Society for Biopreservation & Biobanking



BBMRI-ERIC
Biobanking and
BioMolecular resources
Research Infrastructure

Which are the main new requirements impacting the governance of personal data processing in research biobanking under the EU GDPR?

Gauthier Chassang, Biobanques, Inserm, France
BBMRI-ERIC CS ELSI

Europe Biobank Week – 15 sept 2016 - Vienna - Austria

www.bbmri-eric.eu

Governance to comply with the general principles in data processing (in scientific research)

- Data minimisation
- Purpose limitation
- Data storage limitation
- Data integrity (security) and confidentiality
- Accountability
- Data Protection by design and by default

Outline

- Procedure regarding the appointment of a data protection officer (DPO)
- Data Protection Impact Assessment (DPIA) process
- Measures related to personal data transfers

Designation of a Data Protection Officer (DPO) by the data controller

Section 4 of the GDPR

- New obligation where the core activities of the controller or the processor consist of:
  - processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  - processing on a large scale of sensitive personal data.
- Can be internal or external to the concerned body
- Designation based on professional qualities and expert knowledge of data protection law and practices

- Tasks:
  - to inform and advise the controller or the processor on their obligations and train staffs
  - to monitor compliance and report to the highest level of the controller/processor's organisation
  - to cooperate with the NDPA as a contact point
  - to assist the controllers/processors in the DPIA
- Aims at building an independent close-to-actors data protection governance system

- The DPO shall benefit from sufficient resources to exercise its tasks with controllers/processors
- The number of DPOs must be adequate and take into account the size and organization of the bodies for which they will operate / has to remain available
- The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks

…but DPO liability still unclear – shall be specified by EU or Member States laws.

Data Protection Impact Assessment (DPIA) Art.35

- The GDPR abolishes the obligation to systematically declare any kind of personal data processing in favor of the sole declaration of the processing likely to result in a high risk to the rights and freedoms of data subjects
- DPIA aims in particular situations where :
  - New technologies are used (full genome sequencing?)
  - Special categories of data are processed on a large scale (biobanking; cohorts)
  - Processing consists of a profiling on which decisions that produce legal effects are based

The DPIA report shall contain at least:

- a systematic description of the envisaged processing operations and of its purposes; and
- an assessment of the necessity and proportionality of the processing regarding its purposes; and
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure personal data protection in compliance with this Regulation

- The controller shall consult the National supervisory authority (NDPA) prior to processing where a DPIA indicates that the processing would result in a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation.
- The NDPAs shall establish and publish lists of processing for which a mandatory DPIA is required

International data transfers

- Data transfer = export to non-EU country
- 3 situations are planned under the GDPR to transfer personal data abroad (unspecific to scientific research settings)

1- Adequacy decision from EC

- An adequacy decision:
  - Recognises that a third country legal system ensures an adequate level of data protection in terms of data subject rights and effective legal remedies for data subjects;
  - Allows the free movement of personal data with the third country
    - even though, in the field of scientific research using personal sensitive data it is always recommended to frame the exchange with a tailored contract

2- Existence of appropriate safeguards

- Legal instruments **with binding and enforceable commitments** of the controller or processor in the third country to apply the safeguards and respect data subjects' rights

Without prior authorisation from the competent NDPA in the EU if partners use:

- Standard data protection clauses for data transfers approved by the EU Commission or an NDPA; or
- Approved Binding Corporate Rules Article 47; or
- Approved Code of conducts Article 40; or
- Approved certification mechanism Article 42.

With prior authorisation from the competent NDPA in the EU if partners set up:

- Special data protection clauses not using approved standards; or
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
- New Binding Corporate Rules

3- Other legitimate legal grounds

In the absence of of an adequacy decision and appropriate safeguards a transfer of personal data to a third country shall take place only if:

- the data subject has explicitly consented to the transfer, after information on the possible risks of the transfer due to the absence of previously cited elements;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- […]

What is inside an MTA/DTA?

- ✓ Parties
- ✓ Object of the transfer
- ✓ Purpose(s) of the transfer
- ✓ Organisation of the data flows
- ✓ Obligations of the parties (with legal/ethical references)
- ✓ Framing of onward transfer
- ✓ Financial provisions: Intellectual property (where relevant – not on personal data) – benefit sharing provisions
- ✓ Fate of the data once processed for the defined purpose(s)
- ✓ Duration of the contract
- ✓ Dispute resolution and applicable law

Conclusion

- Data protection governance mechanisms will need to be assessed and updated
- The GDPR aims to reinforce « the tissue » of data protection through capacity building within the organisations and the promotion of self-regulation
- The GDPR reinforces data protection abroad with measures/rights that shall move with the data, including outside EU
- Investments will probably be necessary but they should be beneficial on the long-run as a high level of data protection is a factor of quality and trust and as it is mostly about creating internal capacities

THANK YOU VERY MUCH FOR YOUR ATTENTION !

Gauthier Chassang: gauthier.chassang@bbmri-eric.eu

BBMRI-ERIC
Neue Stiftingtalstrasse 2/B/6
8010 Graz
AUSTRIA
+43 316 34 99 17 – 0
contact@bbmri-eric.eu

www.bbmri-eric.eu