Obligations of a controller –
A walk through the GDPR

Regina Becker
ELIXIR-LU

ELIXIR AllHands TeC Meeting
6. June 2018
First things first...

The messenger requests that she please not be shot.
The heart of the GDPR — The most important principles

**Lawfulness**
Art. 6 Legal Basis
Art. 9 Special categories of data
Art. 44-49 Transfer to third countries or international organisations

**Fairness**
Art. 5.1 (b) purpose limitation
Art. 5.1 (c) data minimisation
Art. 5.1 (d) accuracy
Art. 5.1 (e) storage limitation
Art. 5.1 (f) integrity and confidentiality
Art. 16-21 data subjects’ rights

**Transparency**
Art. 12-15 data subjects’ rights, Art. 30 Records of processing

**Art. 5.1** Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject
(‘lawfulness, fairness and transparency’)

**Art. 5.2** The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).
The GDPR for controllers

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

➔ In the following:
A compendium of the GDPR provisions most relevant for controllers in research
Compliance with GDPR
— Appropriate organisational and technical measures

Art. 24 Responsibility as a controller

Art. 24.1 • Implement technical and organisational measures for compliance with GDPR

Art. 24.2 • This includes data protection policies

Art. 25 Privacy by design and default

Art. 25.1 • Implement data protection principles such as pseudonymisation and data minimisation

Art. 25.2 • Ensure that, by default, only data necessary for each specific purpose of the processing are processed
  - Amount of data collected (only data necessary)
  - Extent of data processing (only necessary processing)
  - Storage period: as short as possible (also for parts of data)
  - Accessibility: limit to people needing access
Additional stakeholders  
— Joint / shared processing

Art. 26 Joint controllers

Art. 26.1 • Determine respective responsibilities for compliance with GDPR, in particular as regards the exercising of the rights of the data subject

Art. 26.3 • Irrespective of Art. 26.1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers

Art. 28 Processor

Art. 28.1 • Use only processors providing sufficient guarantees to implement appropriate technical and organisational measures

Art. 28.3 • Content of contract and mandatory stipulations(!)
Obligation as processor – Art. 28
— Processing must be governed by contract

Content

• Subject-matter and duration of the processing, nature and purpose of the processing, type of personal data and categories of data subjects and obligations and rights of the controller.

• Obligations of processor
  - Process the personal data **only on documented instructions** from the controller
  - Ensure authorised persons **committed to confidentiality**
  - Take all **(security)** measures required pursuant to **Article 32**
  - Engage another **(sub-)processor** only with approval of controller
  - Assist the controller in compliance with **data subject requests**
  - Assist controller in **legal obligations** pursuant to Articles 32 to 36
  - **Delete or return** all the personal data after the end of services
  - Allow for and contribute to **audits**
Documentation obligation — Record keeping following Art. 30.1

Content of processing records

• **Name** and **contact details** of **controller** and, where applicable: joint controller, **representative** and **data protection officer**
• **Purposes** of the processing
• **Categories of data subjects** and **categories of personal data**
• **Categories of recipients** to whom data have been or will be disclosed including recipients in third countries or international organisations
• Transfers of personal data to a **third country** or an **international organisation** (where applicable) **including safeguards**
• Envisaged **time limits** for erasure of different categories of data
• General description of the technical and organisational **security measures**
Security of processing
— Security measures

Art. 32.1  • Measures balance the
  - Costs of implementation
  - Nature, scope, context and purposes of processing
  - Risk of likelihood and severity for the rights and freedoms of natural person

• Measures include among others
  - Pseudonymisation and encryption
  - Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
  - Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures
  - Ensure compliance of staff
Security of processing
— Additional requirements

Art. 32.3 • Assess the appropriate level of security considering accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Art. 32.3 • Ensure that any natural person acting under the authority of the controller who has access to personal data does not process them except on instructions from the controller.
Notification of a data breach
— Destruction, loss, alteration, disclosure, access

Art. 33.1 • Notify supervisory authorities within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Art. 33.3 • Content of notification
- Nature of the breach,
- Categories and approximate numbers of data subjects concerned
- Categories and approximate number of personal data records
- Contact point where more information can be obtained
- Where appropriate: measures taken

Art. 34.1 • Notify data subject if breach is likely to result in a high risk to the rights and freedoms of natural persons

Art. 34.3 • Exemption if measures render data unintelligible (e.g. encryption), measures taken remove risk or disproportionate effort (still requires public communication)
Data Protection Impact Assessment (DPIA) — Risk assessment and corresponding impact

Art. 35.1 • DPIA necessary if processing is likely to result in a **high risk** to the rights and freedoms of natural persons

Art. 35.3 • In particular: if processing **special categories of data** (i.e. health/genetic) on a large scale

Art. 35.7 • **Content** of DPIA
- Description and purpose of processing,
- Assessment of **necessity** and **proportionality** of processing
- Assessment of **risks** to the rights and freedoms of data subjects
- Measures to **address the risks**, including **safeguards**, security measures and mechanisms to ensure protection of personal data

Art. 36.1 • **Prior consultation of Supervisory Authority** needed if processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk

Recital (94) • **Risk cannot be mitigated** by reasonable means in terms of available technologies and costs of implementation
Data Protection Officer (DPO) — A data protection “authority” inside your organisation

Art. 37.1 • A DPO needs to be designated where
- Processing is carried out by a public body
- Core activities consist of processing on a large scale of special categories of data

Art. 37.6 • DPO may be staff member or external consultant

Art. 37.7 • Contact details for DPO need to be published

Art. 39.1 • Tasks of the DPO
- Inform and advise on the obligations pursuant to the GDPR and to other Union or Member State data protection provisions
- Monitor compliance with GDPR, national provisions and institutional policies including assignment of responsibilities, training and audits
- Provide advice on DPIA and monitor performance
- Cooperate with Supervisory Authority and act as contact point for them
Practical discussion...  
— More practical use cases, tools and solutions...

Next presentation / Niclas Jareborg
• Security measures

AllHands Meeting
• Beacon workshop (Thursday)
• Galaxy workshop (Thursday)

Future ELIXIR Data Protection Working Group
• To be applied for in today’s Head of Nodes meeting

Previous events
• Webinar  
  https://www.elixir-europe.org/events/webinar-gdpr
• GDPR Workshop in Brussels

Summary
THANK YOU!