GDPR

General Data Protection Regulation

Marc Rosseau
Data Protection Officer

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with the regard to the processing of personal data and on the movement of such data, and repealing Directive 95/46/EC

- 28 European Members
- No legislative action needed by member states
- Official law since 25 May 2018

Who is affected ?

- Person = EU Resident (Data Subject)
- (Sensitive) Personal data = any information that can identify a person
- EU resident + personal data = GDPR
- EU Company (Data Controller or Data Processor) + personal data = GDPR
- Paper or digital information there is no difference

Definitions

- Data Subject
- Data Controller
- Data Processor
- Data Protection Authority
- Sensitive Personal Data

When can you process personal data ?

1. You asked (informed consent)
2. Compliancy with a law
3. Contractual obligation
4. Saving somebody’s life
5. Government entity with proper authority
6. You have a reason. A REALLY, really, really good reason

When can you process personal data ? Examples

- You asked (informed consent)
  When you organise an event like this symposium. You need a consent to further process the personal data of the attendees. The consent must be an active consent. Opt-out is no longer an option.

- Contract with the data subject.

Need Purpose

- The specific purpose of the processing activities
- When you describe your purpose, the data subject has to understand (transparency)

Don’t get greedy

- Only use the information you need for the purpose you defined
- If you can’t define a purpose you don’t need the data

Try and make sure you are using accurate data

- Where necessary, kept up to date
- Every reasonable step must be taken to ensure that personal data that is inaccurate, is erased or rectified without delay

Don’t keep it longer than you need

- No longer than necessary for the purpose you described
- As described by law : medical records 30 years after last consult
- When you discard data (paper or digital) make sure you take appropriate operational measures

Don’t lose the data or give access to someone who shouldn’t have

- Keep track of by Who, When, Why the data is accessed
- When you lose data or someone has access to data who hasn’t got the necessary permissions to see or access the data, you have a data breach.
- Examples :
  - Screenshot with data
  - Unencrypted mail with wrong email address
- When you have a breach you have to inform the Data Protection Authority (DPA) within 72 hours after notification of the breach. Every data subject involved in the breach has to be notified. Official procedure isn’t available at the moment

Don’t lose the data or give access to someone who shouldn’t have

- When taken the appropriate measures you don’t have to notify the DPA or the data subject.
- Encrypt the data !!!
  - When you use mobile data carriers encrypt them.
  - When using email services make sure that your data is encrypted during transit (by the email services (TLS))
  - When using Skype, WhatsApp, … Make sure that your data is encrypted during transit (these services support encryption during transit)
- Encrypt your laptop, smartphone, USB- key or HD
- Make sure that employees know how to handle removable media. Make sure you document it and start user awareness
- When using cloud services encrypt your data. Use boxcryptor or other applications

Don’t lose the data or give access to someone who shouldn’t have

- Use pincode or password on your mobile device
- When using cloud services encrypt your data. Use boxcryptor or other applications. Look for a cloud provider with data storage in Europe

‘The seven basic principles’

- Lawfulness
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Specific requirements

- Transparent, Clear, Plain
- Who processes
- Who else
- Why
- How long
- Individual‘s rights
- Contact information (DPO)

Privacy statement

- Privacy notice with all the bullets from previous slide.
- Make sure the data subject understands the message. Publish it on website (if available) & on paper available at your practice. Just make sure the data subject has access to it.

Register of processing activities

- What ?
- When ?
- How ?
- Who ?
- Why ?
- Where ?
- For how long ?
- Which security measures ?

Register of processing activities

- Private or hospital you have to have a register of processing activities.
- When you are controller and processor you need a register for both activities. You can combine them in one. Advice：use separate registers
- This is one of the core documents for accountability

When you’re third party (processor)

- Acting only on the controller’s written instructions
- Confidentiality
- Security of personal data
- Authorization for using sub-processors
- Assist controller
- Demonstrate compliance
- What happens when contract ends ?

Individual‘s Rights

- When you are a controller
- Transparant information
- Right to access, correction, erasure
- Data portability (marked copy)
- Right to object
- Right not to be subject to automated decision making

Protect data, analyse risks

- Appropriate technical, organisational, operational measures
- Risk based approach : identify and treat
  - Full organisation
  - Specific process

Assign a DPO

- Expert knowledge on data protection principles
- Internal or External to the organisation
- DPO for a group or a single organisation
- No exact quantification when you need one. Hospitals' ‘large amount of structured data’ needs a DPO.
- Private practice (general practitioner) doesn’t need a DPO.
- Advice : a DPO can be DPO for several small organisations he/she can assist in compliancy with the law, answer questions from DPA and data subject.

Inside or Outside the EU

- Inside is the easiest solution
- Outside the EU
  - Adequacy decision (Privacy Shield)
  - Standard contractual clauses
  - Binding Corporate Rules
  - Just send enough data for diagnosis, if possible no personal data

DPA

- Cooperate
  - Complaints
  - Audit
- Follow up on orders, warnings or restrictions imposed by

- Inform
- Maintain a register
- Respect individual's rights
- Manage third parties, processors
- Protect data and analyse risks
- Notify DPA and the individual of a data breach
- If needed assign a DPO
- If possible keep data inside the EU
- Play nice with the DPA
- Document, document , document it’s the keystone for accountability