GDPR – what’s all the fuss about?

Aly Talen

genae
Disclosure

Speaker name:
   Aly Talen

I have the following potential conflicts of interest to report:

☐ Consulting
☐ Employment in industry
☐ Stockholder of a healthcare company
☐ Owner of a healthcare company
☒ Other: co-founder of genae

☐ I do not have any potential conflict of interest
Background

1995: EU Data Protection Directive
- National legislation → EU differences
- Data breaches
- Court cases, eg the Google case (right to be forgotten)
Background

Publication of the General Data Protection Regulation (GDPR) in 2016

Into force on 25-May-2018
And then....
It’s about European Citizens

ABOUT US
GDPR enforcement

Harmonization across and beyond the EU

- Some points are left to possible national laws, eg age to consent can be lowered

Non-EU entities must comply with the GDPR when dealing with data of EU citizens

- One single supervisory authority though
GDPR definition

Personal Data definition

- any information relating to a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Example: IP address is regarded Personal Data
GDPR – main aspects

Rights of Individuals

- Right to Erasure or Right to be Forgotten
  - Provided certain grounds apply: eg the data is no longer necessary in relation to the purposes for which it was collected

NOTE: clinical trial data cannot be erased when this may endanger their or other people’s health or life
Dutch surgeon wins landmark 'right to be forgotten' case

Ruling will ensure doctors no longer judged by Google on fitness to practise, lawyer says

A Dutch surgeon formally disciplined for her medical negligence has won a legal action to remove Google search results about her case in a landmark “right to be forgotten” ruling.

The doctor’s registration on the register of healthcare professionals was initially suspended by a disciplinary panel because of her postoperative care of a patient. After an appeal, this was changed to a conditional suspension under which she was allowed to continue to practise.
GDPR – main aspects

Rights of Individuals

- Right to be Informed
  - Who is collecting your personal data and what’s the purposes for which data controllers are processing it
Here is a list of your Facebook information that you can access at any time. We've categorized this information by type so you can easily find what you're looking for. Our Data Policy has more information about how we use your information, how it's shared and how long we retain it. It also outlines your rights and how you can exercise them, and how we operate and transfer your information as part of our global services.

You can choose to download your information if you'd like a copy of it.

Your Information

- Posts
  - Posts you've shared on Facebook and posts you've been tagged in

- Your Posts
  - Photos, videos, text and status updates you've shared on Facebook

- Posts You're Tagged In
  - Posts that people tag you in

- Other People's Posts To Your Timeline
  - Posts other people have shared on your timeline

- Posts Hidden from Your Timeline
  - Posts that you've chosen not to show on your timeline, including posts you've created and posts that other people have created

- Notes
  - Notes you've created or have been tagged in

- Polls
  - Polls you have created
GDPR – main aspects

New roles

- Data Protection Officer (DPO)
- Data Processor
- Data Protection Authority (DPA)
GDPR – main aspects

Fines & enforcement:

- Significantly higher fines
  - €10 million or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.
  - €20 million or 4% of the entity's global gross for violations on the processing (including consent...), data subject rights, and cross-border data transfer
Clinical trial data

! Sensitive data

- Patients must be informed about what data is collected, where it’s stored, who has access, ..
- Transferring data outside Europe, must be according to GDPR legislation for data collected in the EU!
- Data processors need to be assigned to support this process
Summary

Think about the data you have

The data you intend to collect

What you will do with the data

Document the process, what you capture and who will have access to this
GDPR – what’s all the fuss about?

Aly Talen

genae