Lecture 10
Friday, 7 October 2022 15:31

Privacy

multiple definitions possible

more than confidentiality

privacy set boundaries on (governments and) private organizations

there are privacy laws
↳ violations can be costly
↳ financially
↳ reputation

there is a huge amount of data collected & stored by organizations

collection + use of data leads to privacy

low balance necessity to process information with privacy concerns

OECD fips

information practices
collection limitation
data quality
purpose specification
use limitation
security safeguards
openness
individual participation
accountability

GDPR

data protection by design
responsibility and accountability
data breach notification within 72 hours
sanctions

personal data → can be used to identify individual
pseudonymized data

identificate data → can be used to directly identify an individual

sensitive data: e.g.
DNA
religion
health
sexual orientation
politics

data processing is any action which deals with data

data subject is the person to whom the data refers
data controller defines purpose for which and manner in which data is used/stored
data processor processes data on behalf of the data controller

The purpose is the rationale of the processing, on the basis of which all the actions and treatments have to be performed

purpose management
purpose determination
purpose control (verification of whether data is used for stated purpose)

consent should be informed, unambiguous and freely given

opt-out
opt-in
double opt-in → also confirm e.g. recipient phone number or mail address

data should be deleted when retention period expires

an obligation is a mandatory requirement to be fulfilled
↳ impose constraints on how data may be used
↳ post-update: delete after retention period expires

privacy principles

fair and lawful processing
purpose specification
consent → without consent:
- to perform contract with data subject
- to comply with legal obligation
- to protect vital interests
- to perform a task in the public interest
- "legitimate interests"

minimality → includes deletion after retention
limited disclosure
information quality
data subject's control
security
information security

data subject rights

to know which information is collected/used/disclosed
to know who is responsible for handling information

right to erase collected information
right to block information
right to revoke consent