General Data Protection Regulation: Sensitive data

Nataliia Bielova

nataliia.bielova@inria.fr

GENERAL DATA PROTECTION REGULATION

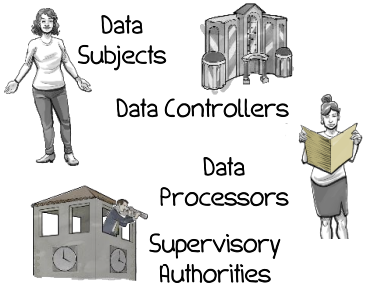
GDPR

TERRITORIAL SCOPE

EU Establishments

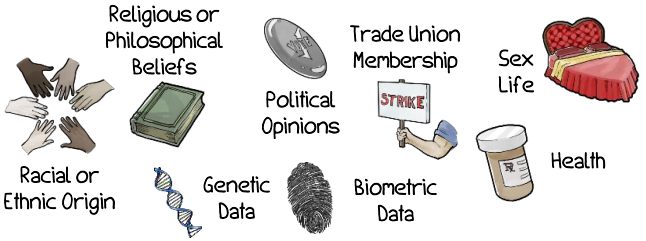
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA

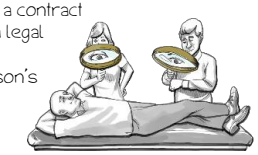
SENSITIVE DATA



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



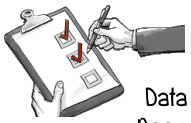
CONSENT

Consent must be freely given, specific, informed, and unambiguous.

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

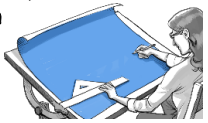
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

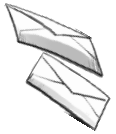


Data Impact Assessment
For high risk situations

Data Protection by Design
built in starting at the beginning of the design process



DATA BREACH NOTIFICATION

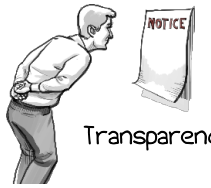


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."

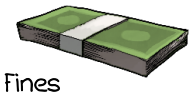
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT



Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

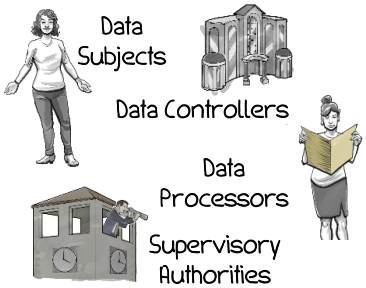
GDPR

TERRITORIAL SCOPE

EU Establishments

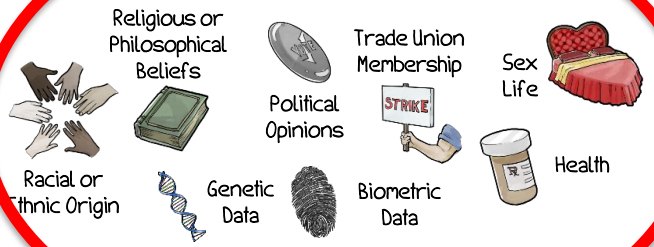
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA

SENSITIVE DATA



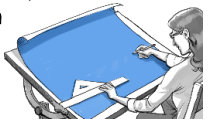
RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

Data Protection by Design
Built in starting at the beginning of the design process

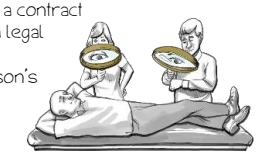
Data Impact Assessment
For high risk situations



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

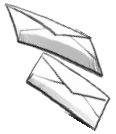
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

Consent must be freely given, specific, informed, and unambiguous.

DATA BREACH NOTIFICATION

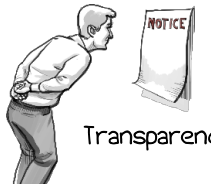


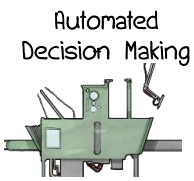
A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

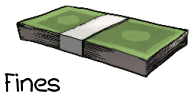
RIGHTS OF DATA SUBJECTS





"Right not to be subject to a decision based solely on automated processing, including profiling."

ENFORCEMENT



Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY 2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

SENSITIVE DATA

Special Categories of Personal Data Art. 9

racial origin: makes reference to classifications such as skin color, bone structure, facial form, eye color

ethnic origin: sharing a common lineage or heritage, a common history or culture. Can be geographic origin, language or dialect, ideology

political opinions

religious or philosophical beliefs

membership of a **trade union**

genetic data: human tissue cells harvested

biometric data

health data

sex life or sexual orientation

Processing “sensitive” data is prohibited, unless…

• You have a lawful basis for processing under Article 6 (as you would for other personal data) but you must *also* satisfy a condition under Article 9:

- **Explicit consent**
- Employment law
- Vital interests of anyone
- Not-for-profit TU/religious/ political/philosophical groups
- Already in public domain where put by the data subject
- Legal proceedings/advice
- Substantial public interest
- Medical purposes
- Public Health
- Archiving in public interest, scientific/historical research purposes or statistical purposes

Example

An individual signs up for a pregnancy yoga class. The instructor will be processing data concerning their health (ie the fact of their pregnancy along with any information about due dates) and therefore needs both a lawful basis and a condition for processing special category data.

As the instructor needs to process these details to provide the yoga class, the appropriate lawful basis is likely to be 'performance of a contract'.

Although the individual cannot sign up to the class without revealing information about their pregnancy, explicit consent is still likely to be the appropriate condition for processing health data. The processing is objectively necessary to provide the requested class, and the individual has a free choice whether or not to sign up to that class.