The Data Protection Regulation for Europe

Magnus Stenbeck, Karolinska Institutet
Dept of Clinical Neuroscience
and
The Research Data Inquiry (U 2016:04)

The data protection regulation in the EU

Old system
- The 1995 Data Directive
  ➔ Prescribes that member states shall implement laws and regulations in accordance with the directive
- Personal Data Act (1998)
  ➔ Swedish implementation
  ➔ Void by May 25, 2018

New system
- The 2016 General Data Protection Regulation
  ➔ Applies as from May 25, 2018
  ➔ Directly applicable in member states (MS) and associated states (e.g. Norway)
  ➔ Needs additional union or MS legislation
- All national regulation is obsolete/must be removed
- Some Swedish additional laws
- Many modifications of existing regulations
General Data Protection Regulation (”GDPR”)  

- replaces the Personal Data Act (PUL)  
- takes priority over Swedish legislation  
  → PUL was subsidiary (other legislation took priority)  
  → GDPR does not leave space for deviating national rules or special rules in specific subject matter areas  
- But some additional new Swedish legislation is needed  
- many articles refer to the need for union or member state regulation  
- GDPR leaves space for some constitutional rights and obligations

Current legislation which will prevail

- The Freedom of the Press Act  
- The Fundamental Law on Freedom of Expression  
- The Law on Public Access to Information and Secrecy  
- The Ethical Review Act
Some important rules in research not changed by GDPR

- The Law on Public Access to Information and Secrecy
  - Chapter 24, 8 § Statistical secrecy
  - Chapter 25, 1 § Secrecy in health care
  - Differ slightly, but both have "reversed damage requirement"
    - You have to prove that nobody can suffer damage if you release the data to research
  - Chapter 11, 3 § Secrecy is transferred with the data if it will be used for research purposes
- The Law on Ethical Review
  - Review is mandatory when using sensitive personal data and biological samples from living persons
  - Permission can be granted for research in Sweden

Sweden:
Proposed new legislation

- The Data Protection Law (SOU 2017:39)
  - SOU 2017:39 Ny dataskyddslag
- The Research Data Law (SOU 2017:50)
  - SOU 2017:50 Personuppgifter för forskningsändamål
- Most register laws remain, but must be adapted
  - Ds 2017:40 Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform
  - SOU 2017:66 Dataskydd inom socialdepartementets verksamhetsområde
  - S 2016:04 Biobanksutredningen (proposal due Dec 31, 2017)
Important issues for Sweden in Brussels 2012-2016

- Protect freedom of speech and the principle of public access
  → Outcome: Articles 85 and 86
- Exemptions for archiving, statistics and research
  → Save the population based registers and register based research
  → Outcome: Article 5 b and Article 89
    - Exemption from the purpose limitation principle
- Excessive rules regarding health data used outside the immediate treatment/care context
  → Outcome: removed
- GDPR allows for continued register based research and statistics if it is amended with national legislation

Central concepts

- Personal data
- Special categories of personal data ("sensitive personal data")
- Consent
- Pseudonymisation
- Research purpose
- Safeguard
Personal data

- Personal data
  - any information relating to an identified or identifiable natural person (‘data subject’)
  - an identifiable natural person is one who can be identified, directly or indirectly

- Pseudonymisation
  - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information
  - this additional information is kept separately and protected by subject to technical and organizational measures

Basic principles for personal data processing
Article 5

- Lawfulness, fairness and transparency (openness in relation to the data subject)
- Purpose limitation (Swedish: "finalitetsprincipen")
  - Exemptions for archiving, statistics, research
- Data minimisation
- Accuracy
  - Exemption for archiving
- Storage limitation
  - Exemption if necessary for research
- Integrity and confidentiality (=protect the data)
- Accountability
Personal data processing is legal only when one of these apply  
Article 6

a) Consent  
   or processing of personal data is necessary in order to:
b) Perform a contract  
c) Comply with a legal obligation  
d) Protect the vital interests of the data subject or another person  
e) Perform a task in the public interest  
f) The interests of the controller override those of the data subject  
   → f cannot be used by public authorities  
   ▪ c and e requires a legal basis (new requirement!)

Sensitive personal data (special categories)  
Article 9

▪ Race, ethnicity  
▪ Political, religious, philosophical beliefs  
▪ Trade union membership  
▪ Genetics  
▪ Biometrics for the purpose of identification  
▪ Health  
▪ Sexuality (sexual orientation)
Processing of sensitive personal data

- is forbidden
  → Same as today

- Exemptions if
  → … consent from the data subject .. except where Union or Member State law provide that the prohibition … may not be lifted by the data subject
    - Sweden: the law prescribes mandatory ethical review
  → processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)
    - Must be based on union or MS law which is proportional, and safeguards are required

Consent

Legal definition

- Freely given
- Specific
- Informed
- Unambiguous
- A statement or a clear affirmative action
- and for sensitive personal data: Explicit

- The controller shall be able to demonstrate that the data subject has consented
- Consent can be withdrawn at any time
  → for subsequent processing
Legal basis for public authorities

- Consent?
  - Sometimes, but questionable

Recital 43:
"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."
  - If a public authority wants to use consent it must be able to show that it is freely given

- Performance of a task in the public interest

Safeguards

- Mandatory in research
- Proposed in the Swedish research data law
  - Ethical review
    - Only for sensitive data
  - Pseudonymisation (or similar level of protection)
  - Right to opt out (if possible)
- Other possibilities
  - Organisational solutions
    - organisationally separated personal data processing
  - Technical solutions
    - Federated data, remote access, other distributed solutions, encryption, logging, safe authorisation procedures, etc.
Rights of the data subject

- In principle similar to current rules, but much more detailed
  - Information (Art 12-14)
  - Art 15: Right of access ("register excerpts")
  - Art 16: Right to rectification
  - Right to erasure ("right to be forgotten") restriction or objection to processing (Art 15-18, 21)
- In most of these cases, there are exemptions
  - if necessary for research or
  - impossible to fulfil

Accountability of the controller

- The controller is responsible for implementing technical and organisational measures to ensure that processing of personal data follows this regulation
- This may include using approved rules of conduct (Article 40) and certification procedures (Article 42)
- It may also include a data protection impact assessment
- Possible fines for breaches:
  - administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher
  - The Data Protection Inquiry has proposed an upper limit of 20 000 000 SEK for public authorities
What is needed before May 25, 2018?

- Analyse whether the processing of personal data in your organisation is (still) legal
  - You have to be able to prove this by proper documentation
    - Document the existing processing (including storage of old data)
    - Did you obtain consent according to the legal definition?
    - Can you show documentation of this?
    - Can you document that your processing is in accordance with the law defining a public interest?
    - Analyze the documentation system guided by GDPR

- Design organizational processes
  - Ensure rights of the data subject
  - Handle data protection incidents