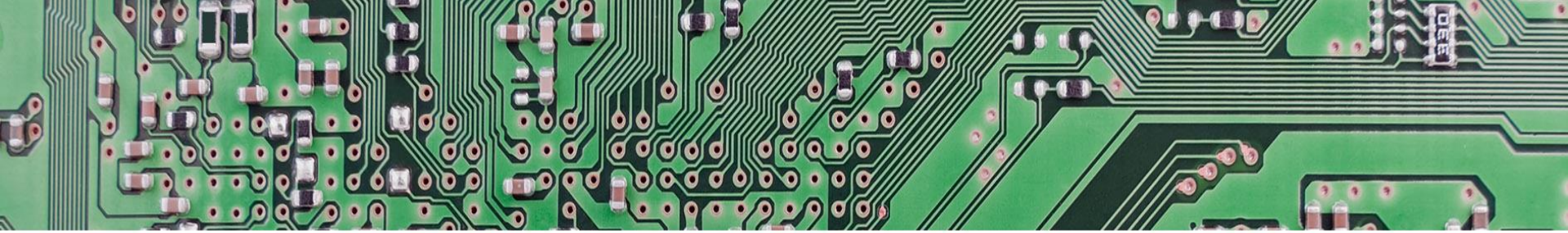

UiO : USIT

Introduction to privacy law

- Better safe than sorry

Research Bazaar 2018

February 8th 2018

Asbjørn Tingulstad Hem
Legal advisor USIT


~ Data protection law ~
© 2008 Alexis Andrews IndianCreekBooks.com

Todays agenda – an introduction

trying to understanding data protection law

- What is the right to privacy?
- Principles of data protection law
- Applicable privacy law for researchers at UiO
- GDPR (coming laws)
- Important terms and definitions
- Research based on personal data – How to
- GDPR for researchers

What is the right to privacy?

- The right to privacy concerns your right as individuals to influence and decide the use of your personal data.

- Your money vs your data

- Building blocks of privacy law
  - The right and possibility to self-determination and codetermination
  - Right to be in control of how your data is used

- Principles
  - Purpose limitation, lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, integrity, confidentiality, accountability

Principles relating to processing of personal data – GDPR article 5.

- 1.Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency**’); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘**purpose limitation**’); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’); 4.5.2016 L 119/35 Official Journal of the European Union EN (1)Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1). (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘**storage limitation**’); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’). 2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability**’).

Applicable law

- **Today: Norwegian Personal Data Act (2000) (1995 EU Privacy Directive)**

  + different set of laws

- **In 4 months from May 25th 2018: The EU General Data Protection Regulation (GDPR) and new Norwegian Personal Data Act**

  + different set of laws

New obligations?

- Old vs. new regulation

✓ Right to be forgotten
✓ Right to withdraw consent
✓ Right to information

– New
  - Right to object
  - Right to data portability (transfer of data)

Important terms and definitions

- Personal data (vs. anonymous data)
- Special categories of personal data
- Data subject
- Processing personal data
- Data controller
- Data processor
- Consent

  - freely given, specific, informed and unambiguous

Data protection law for researchers

- Jeg er forsker (http://www.uio.no/for-ansatte/arbeidsstotte/personvern/forsker/)
  - The university guidelines (in Norwegain only)

- You do not own someone else's personal data
  - you can be allowed to borrow it on certain conditions

- **Step 1**: Planning your research and planning the collection of data
- **Step 2**: How to collect it, and what to do once you have it, or once you are processing it or analysing it.
- **Step 3**: What to do after your conclusion

Step 1: Planning your research

Required data – purpose limitation, data minimisation

- What purpose is to be fulfilled?
- Which data is needed? Categories of data? How will it be collected? Respondents?

Legal basis – lawfullness, transparency, fairness

- Consent from the data subject

✓ Freely given
✓ Informed
✓ Clear and plain language
✓ Specific
✓ Unambiguous
✓ Clear and affirmative action
✓ Documented (written)

- Consent form and information to the data subject

Application to NSD/REK/DPA

- Research? - NSD
- Medical and health research? – REK
- Not them? - Data Protection Authority

Choice of processing systems/applications/services

- Calculations?
- Storage?
- Online questionnaire?

- Which systems can UiO provide?
  - TSD
  - Questionnaire application
  - …and more

- Data processor agreement
  - To ensure your control
  - Process data according to your instructions only

Risk analyses
- confidentiality, integrity, accuracy

- Can you still allow yourself to process the data needed?

What are the risks in processing the data?

- Leak
- Lost storage device
- How special is the data in question?
- Who will have access? Can they be trusted?
- Stored in a cloud or desk top drawer?

- Neccessary precations and actions

Step 2: Collection and processing data

Storage limitation, transparency, purpose limitation, fairness

- Collection and during analyses
  - The consent and necessary information
  - Answer to your data subjects
  - Delete data or anonymise them if consent is withdrawn
  - Ensure original purpose – New purpose? Requires consent
  - Notification of personal data breach

- Keep track: maintain integrity, confidentiality and accuracy

Step 3: Having concluded your research

- Data analyses finished
  - Erasure of data
  - Anonymisation of data
  - Publication of research
  - Transfer of data
- Remember the results are yours, the data is not.
  - You have borrowed them.
- Follow up – Report to NSD / REK / DPA

(Michael Rosskothen / Shutterstock)

GDPR – Implications for researchers

- What we can assume

  - Awareness
    - more critical/interested data subjects
    - more data subjects willl exercise their rights

- Application to NSD/REK/Norwegian Data Protection Authority substituted by an extensive data protection impact assessment

The principles of article 5

- Purpose limitation, lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, integrity, confidentiality, accountability


principles
~ Data protection law ~
© 2008 Alexis Andrews IndianCreekBooks.com