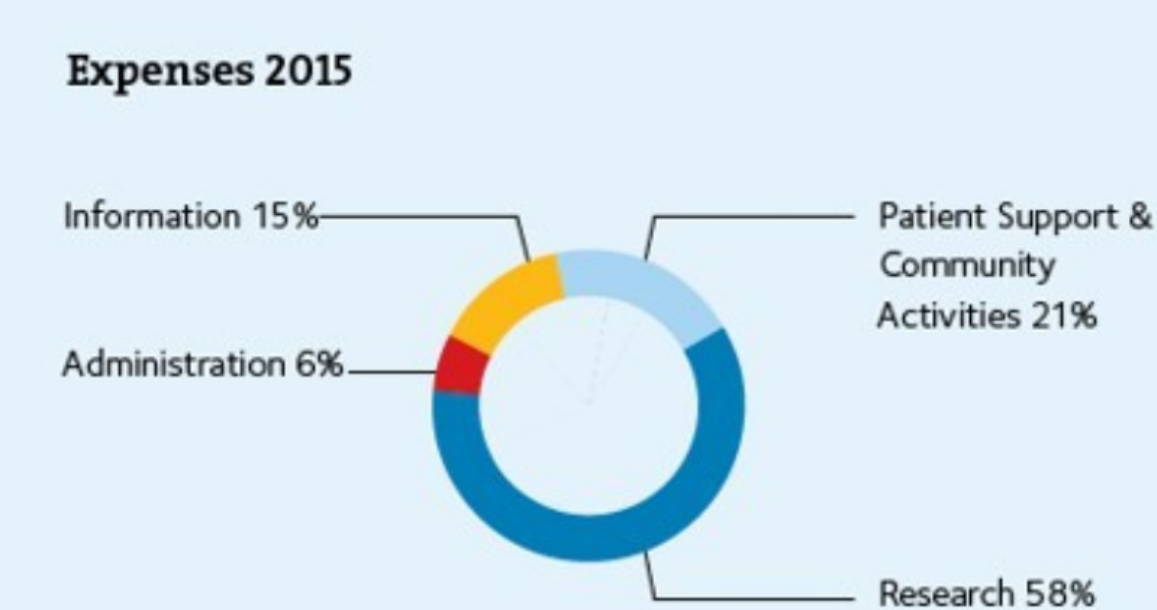
Register based research and the impact of the new EU Data Protection Regulation

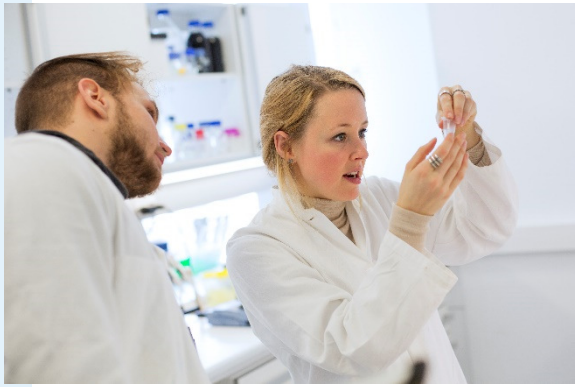
Mette Rye Andersen, Danish Cancer Society
LuxCLIN 30 May 2017

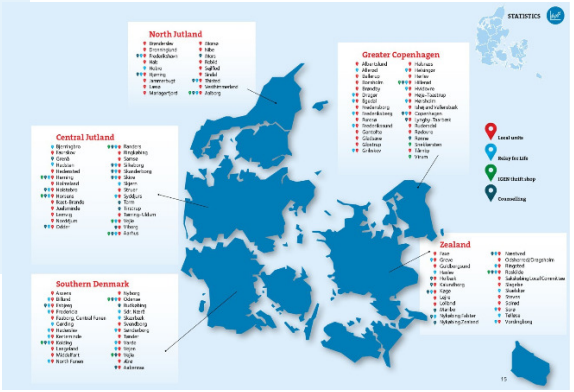
Outline

- Brief introduction to the Danish Cancer Society
- Key elements and articles of the EU GDPR
  - What is business as usual?
  - What is new?
- Conclusions

Danish Cancer Society







Purpose of the data reform

Harmonize data privacy laws across Europe

Protect and empower all EU citizens data privacy

Simplify the regulatory environment for business (digital economy)

Replace the Data Protection Directive 95/46/EC

Will research benefit from data protection harmonization?

EU Data Protection Regulation

Proposed January 2012

Approved 14 April 2016

Applies from 25 May 2018

Does not require any enabling legislation to be passed by Member State governments

- Though there are possibilities to adopt Member State legislation

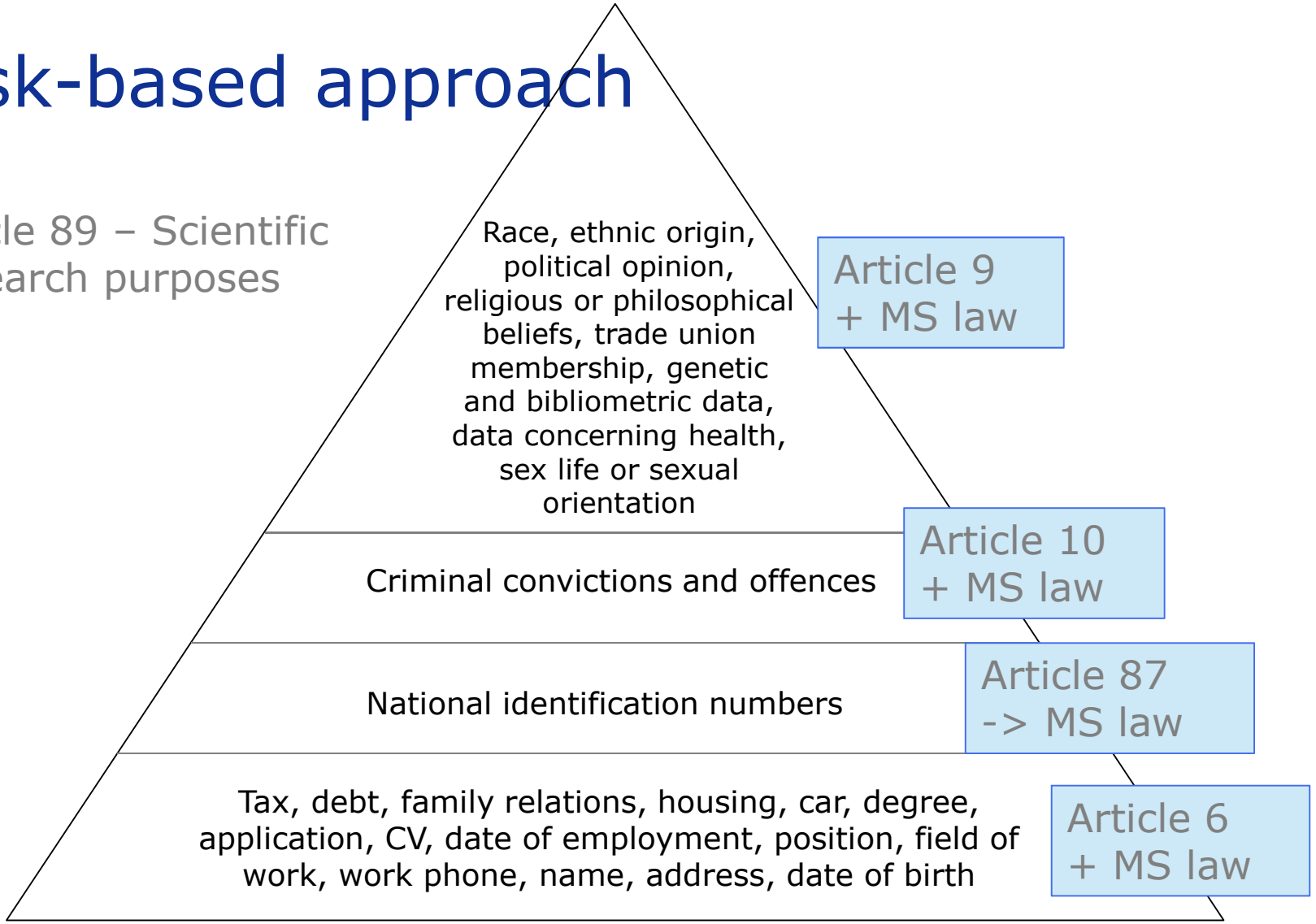
Fundamental right

- The protection of natural persons in relation to the processing of personal data is a fundamental right (recital 1)

  - Data protection is no absolute right
  - Regulation leaves room for balancing interests of the public against those of the individual
  - The value of scientific health research is acknowledged

Risk-based approach

Article 89 – Scientific Research purposes



Principles (article 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

- Accountability

Controller shall be responsible for, and be able to demonstrate compliance with these principles

Lawfulness and health data (article 9)

- Consent as legal basis
  - Explicit and written consent of the data subject
    - Broad consent for certain areas of scientific research (recital 33)
  - Unless processing for purposes of
    - Public health
    - Preventive or occupational medicine
    - Medical diagnosis
    - Provision of health care or treatment
    - Scientific research purposes (article 89)

    Depending on MS law – further conditions, including limitations can be introduced

Research purposes (article 89)

- Use of anonymous or pseudonymous data where possible
- Technical and organisational measures to protect data and ensure data minimisation

Member States may introduce exemptions from:

- Right of access by the data subject (article 15)
- Right to rectification (article 16)
- Right to be forgotten (article 17)
- Right to restriction of processing (article 18)
- Notification obligation (article 19)
- Right to data portability (article 20)
- Right to object (article 21)

Purpose limitation and the interest of the data subject (recital 159)

- *[..] If the results of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.*

Codes of conduct (article 40)

Various processing sectors are encouraged to draw up codes of conduct intended to contribute to the proper application of the regulation – taking into account sector specific features and needs.

Example of initiative:

BBMRI-ERIC®
gateway for health

Security of data

- Security of processing (article 32)
  - Privacy by design (article 25)
- Data Protection Impact Assessment (article 35)
  Processing on a large scale of special categories of data (e.g. health data)
- Data Protection Officers (article 37)
  inform and advice
  monitor compliance
  cooperate with supervisory authority
  act as contact point
- Demonstrate compliance
  map data and data processing
  adopt internal policies and adopt measures
  audits
  internal education and awareness

Alerts, corrective powers and sanctions

- Notification to supervisory authority (Article 33)

  without undue delay and within 72 hour

- Notification to the data subject (Article 34)

  without undue delay when at high risk to the rights and freedoms of natural persons

- Powers of supervisory authority (Article 58)

  Issue warnings

  Reprimands

  Give orders to comply with specific provisions

  To impose a temporary or definitive limitation or ban on processing

- Fines and penalties (Article 83 & 84)

  - effective, proportionate and dissuasive

Conclusions

- Public confidence in use of health data for research purposes must be maintained
- The GDPR has failed to harmonize data protection rules across the EU
  - Legal patchwork across EU?
  - To what extend will data sharing and collaboration be possible?
  - Even if business as usual is an option - what will MS politicians decide?
  - Broad consent – interpretation of "research area"?
  - Softening of purpose limitation concerning use of research results?
  - Future level of fines and penalties?
- Controllers and processors should demonstrate compliance – within the next year
- Explore the possibilities of codes of conduct

Questions?