Research data management when working with children and youth

DAY 1

Workshop
Ljubljana, Slovenia
27 – 28 March 2023

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101008589

COORDINATE
COhort cOmmunity Research and Development Infrastructure Network for Access Throughout Europe

Legal grounds for processing personal data

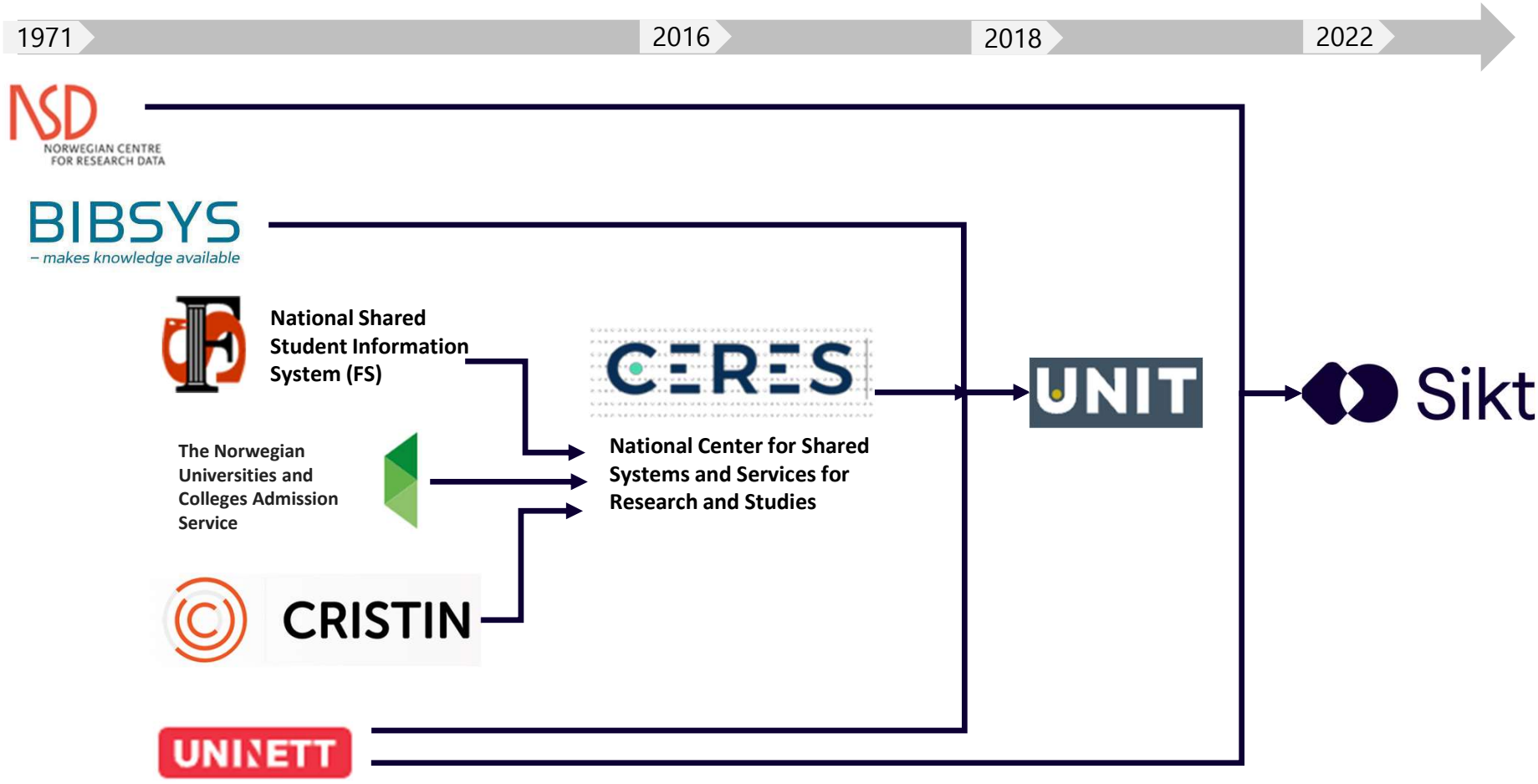
Marianne Høgetveit Myhren, Sikt

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101008589

Workshop
Ljubljana, Slovenia
27 – 28 March 2023

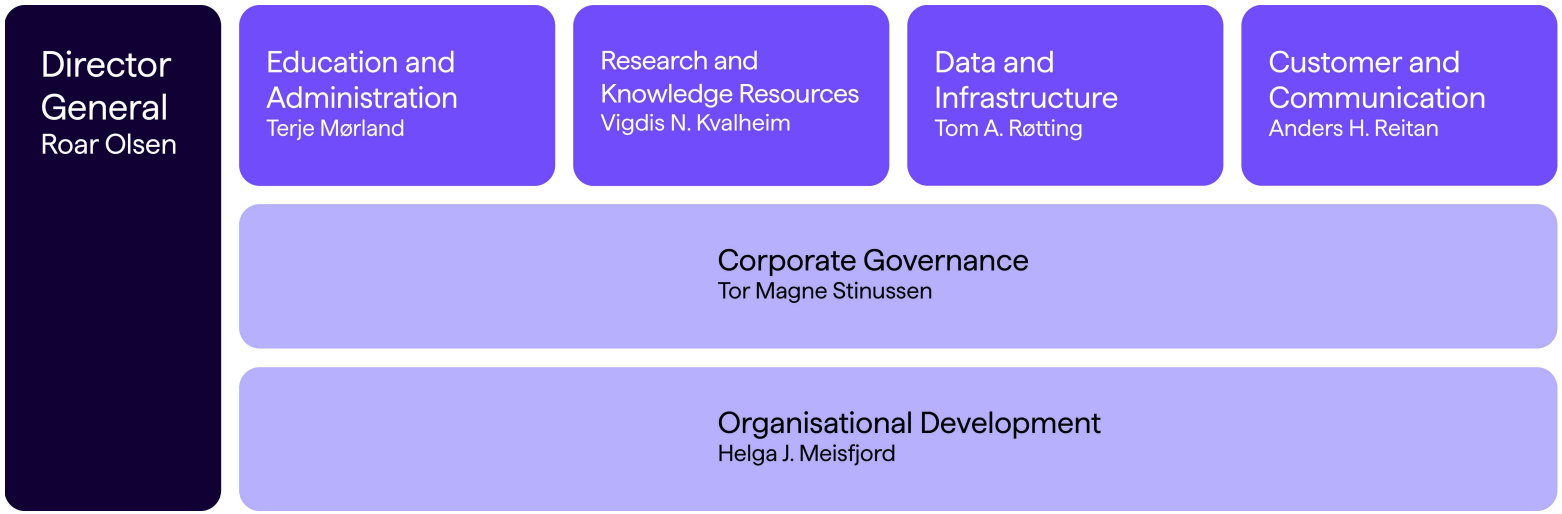
COORDINATE
COhort cOmmunity Research and Development Infrastructure Network for Access Throughout Europe

Sikt (and it's Predecessors)



Sikt - Norwegian Agency for Shared Services in Education and Research

Sikt develops, acquires and delivers services for education and research. In collaboration with our users, we offer a common infrastructure for education and research. The aim is to free capacity for our customers, and to meet overarching goals of digitalisation, data sharing and open research.



Approx. 400 employees

Sikt

Sikt – Research and Knowledge Resources

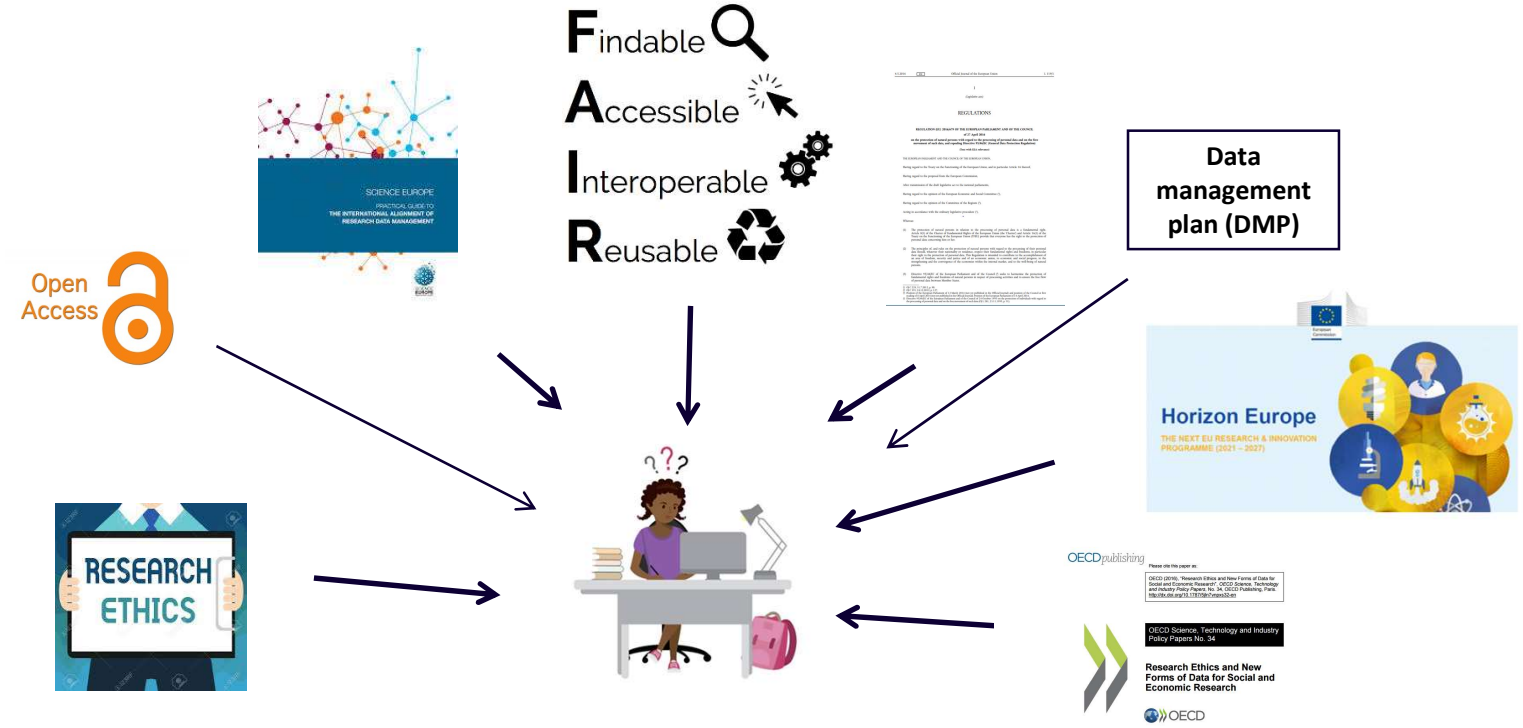
Sikt

Presentation outline

- Landscape
- An overview of important terms
- Principles
- Legal bases
- Children and youth
- Rights
- Data Protection Impact Assessment
- Transfer to third countries

Landscape

"As open as possible and as closed as necessary"



Sikt

Ethics vs law

- An ethical approach helps determine how research **should** be undertaken
- The legal framework specifies what **must or must not** be done to comply with relevant laws.
- Research that does not comply with relevant laws should not be undertaken.
- Even though a project may fall outside the scope of the privacy regulation it's important to remember that ethical guidelines still applies

Relevant legal framework

- The European Convention on Human Rights
- General Data Protection Regulation (GDPR)
- National Constitutions
- National Data Protection Acts
- Statistics acts
- Separate laws/special laws on specific registers and classes of data (e.g. Health registers/Patient Data Laws etc.)
- Intellectual Property Rights (IPR)/Copyright
- Terms of use
- Duty of confidentiality

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

European Convention on Human Rights, article 8.1

Sikt

Key goals of the GDPR

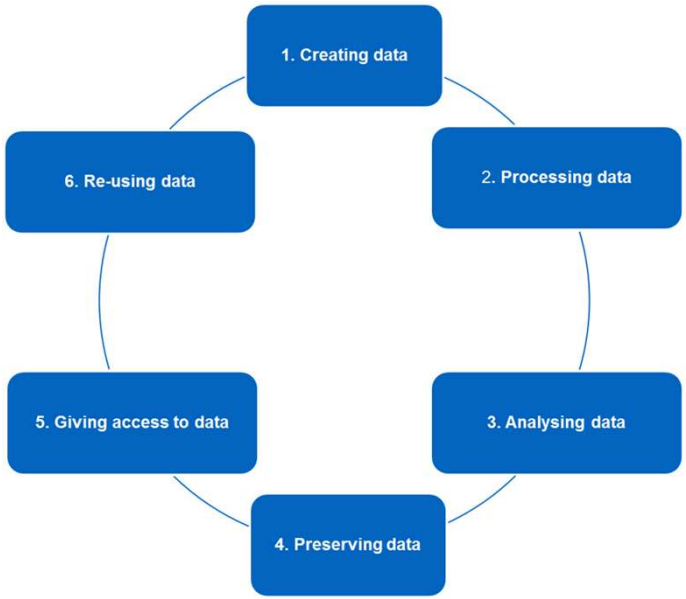
- Make Europe fit for the digital age
- Harmonise the rules across Europe
- Remove barriers to facilitate cross border data flow
- Ensure a high level of data protection in order to provide legal certainty and trust
- Put citizens in control of their data

Special provisions for archiving and research purposes

- Further processing is **not considered to be incompatible** with the initial purposes (Article 5(1)(b)).
- Personal data **may be stored for longer periods** (Article 5 ,1 (e))
- Exemptions from «right to be forgotten» and «right to object»
- Union and Member States may create further derogations from the data subject's rights

Law and legal practice affect all stages of the research data lifecycle

- How are you planning to:
  - Collect data
  - Organise/structure/analyse collected data
  - Store data
- Do you plan to:
  - Share data with others and will they have access (during research project and afterwards)
  - Archive data
  - Reuse data in the future



Sikt

Tip 1: Plan ahead

During the **planning stages** think through the life-cycle of your collected data

Be prepared to collect good research data!

Terms and definitions

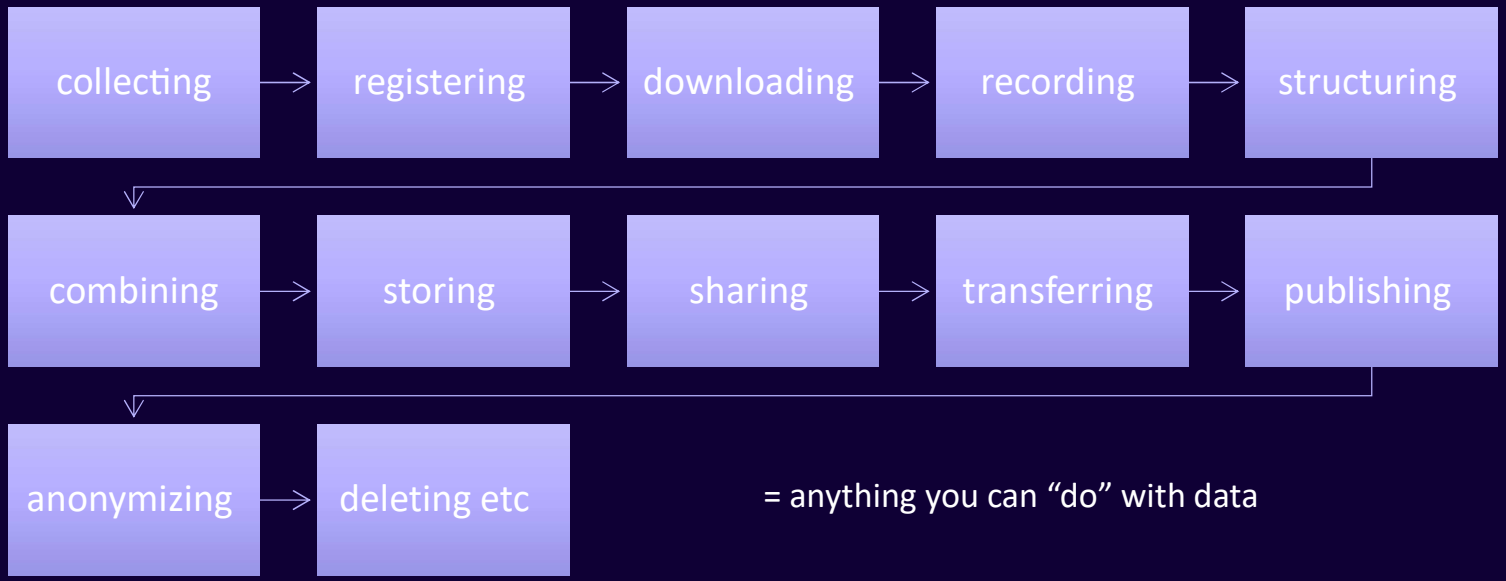
Scope of the GDPR

- **Material:** Processing of personal data by automated means

- **Territorial:**
  - Controller/processor in Europe,
  - or processing of personal data from European data subjects

What is processing?

Processing entails any operation which is performed on personal data, such as…



= anything you can “do” with data

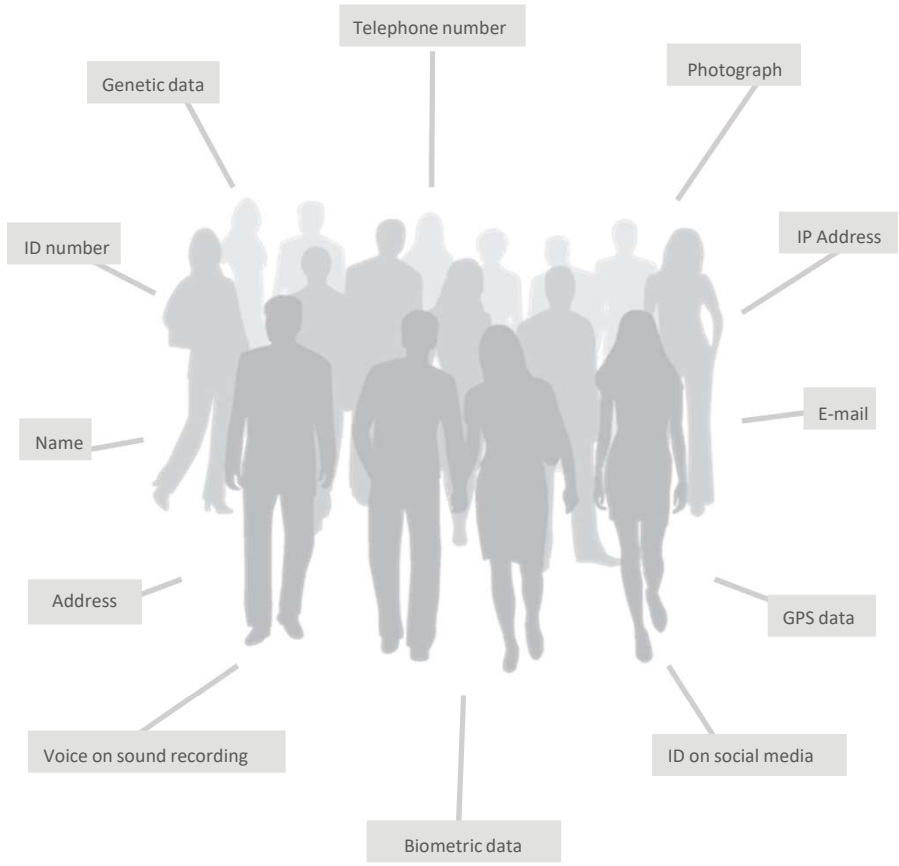
Sikt

Controller and Processor

- **Data controller:** determines the purposes and means of the processing of personal data
- **Joint controller:** jointly determines purposes and means
- **Data processor:** processes personal data on behalf of the controller (for the controller's purposes)

What is personal data?

Any information that can be used (by means reasonably likely to be used) to identify a person **directly or indirectly.**



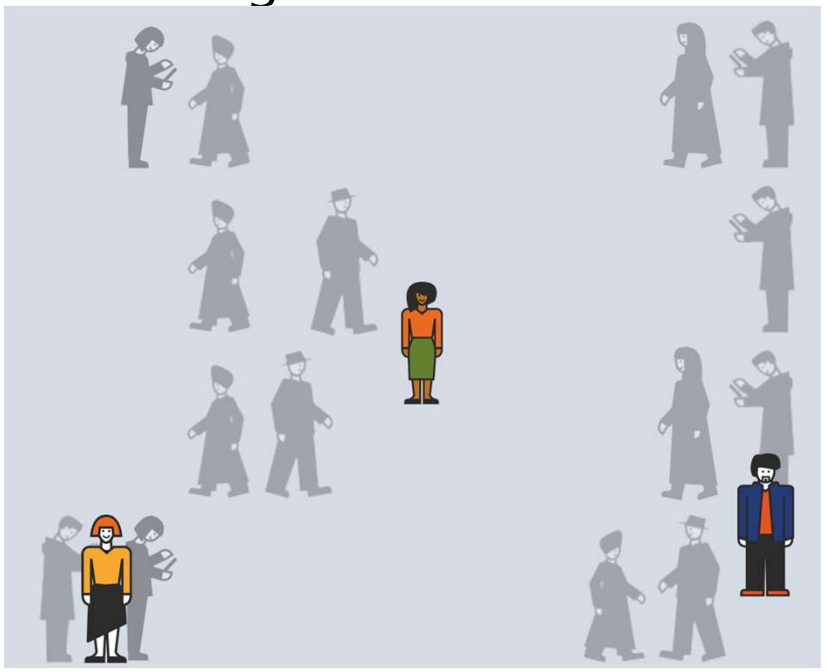
Sikt

Indirectly identifyable personal data

A person can be identified based on a combination of background information/demographic data e.g:

- Gender
- Age
- Occupation
- Place of work
- Address
- Voice recordings
- Photo/video of faces

Etc..



Sikt

Who is this?

Sikt

Sikt

- Male
- Businessman and politician
- PhD in electrical engineering
- Born in 1967
- Member of the Freedom Movement

Sikt

Sikt

Sikt

Special categories of personal data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sex life or sexual orientation
- Criminal offences/convictions

What is anonymous data?

- Information that can in no way be linked to an individual person
  - Directly,
  - Indirectly, or
  - through a list of names/codes (i.e. scrambling key)

Sikt

What is pseudonymous data?

- The handling of personal data in such a way that no individuals can be identified from the data without a "key" that allows the data to be re-identified
  - Involves removing or obscuring direct and indirect identifiers
  - The key must be kept separately and secure
- Pseudonymisation reduces the risks of data handling, while also maintaining the data's utility
- Explicitly encouraged as a security measure
- Pseudonymised data is still considered as personal data!

Sikt

New forms of data - a challenge for the data subjects' confidentiality?

"Privacy as we have known it is ending, and we're only beginning to fathom the consequences" (Enserink and Chin 2015).

Four essential principles to retain trust:

- Transparency
- User control
- Privacy be design
- Accountability

Sikt

Data on third persons

- Third persons are persons that are not included in the sample/are not participating in the project.
- Information relating to third persons is information provided by a data subject that relates to an identified or identifiable third person.
- Examples: when a data subject is asked about their mother's and father's education or country of origin, or when pupils are asked about their teacher's teaching methods.

Case – children

- Research project involving children in kindergarten
- Data is collected from children through research assistants that will ask them questions from a questionnaire
- Special categories of data about health and social benefits
- Data will be collected at a later point from registries:
  - sociodemographic data on parents,
  - data from the children's grades in school at various points (after 5, 10 and 15 years)
- Data will be stored for 20 years in total and shared with other researchers in the EU

Questions for discussion:

- What could a legal ground for conducting the research be?
- What is the best way to provide information to the parents?
- Should the children receive information at some point? When?
- Do you see any ethical, legal or practical challenges here?

Tip 2 – consider three aspects at every stage

1) Principles

2) Legal basis

3) Rights

- then you will have covered what is most important from a data protection perspective

Sikt

7 principles of the GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality
7. Accountability

Lawfulness, fairness and transparency

- Processing of personal data must happen in a *lawful way* and thus have a legal basis which makes the processing legitimate
- *Fairness* means that your actions must match up with how it was described to data subject
- A clear notice/information sheet is what the concept of *transparency* is about

Purpose limitation

- Personal data shall be collected for specified, explicit and legitimate purposes
  - Be specific and clear from the outset why you are collecting personal data and what you intend to do with it;
  - Inform the participants about the purpose of the data collection
- You can only use the personal data for a new purpose if:
  - this is compatible with your original purpose,
  - you get consent,
  - or you have a clear obligation or function set out in law.

"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."

Data minimisation

Ensure that the personal data you are processing is:

- Adequate,
- relevant and,
- limited to what is necessary in relation to the purposes for which they are processed

You should identify the minimum amount of personal data you need to fulfil your purpose.

Accuracy

Personal data shall be:

- 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.

Storage limitations

- Retain the personal data for the necessary period and then erase or anonymise
- You can keep personal data for longer if you are keeping it for public interest archiving, scientific or historical research, or statistical purposes.

search.creativecommons.org/; future.agenda/CC BY-NC-SA 2.0

Sikt

Integrity and confidentiality

- Keep the data secure!

- “in a manner [ensuring] appropriate security”, which include “protection against unlawful processing or accidental loss, destruction or damage”.

search.creativecommons.org/; future.agenda/CC BY-NC-SA 2.0

Sikt

Accountability

- You are responsible for compliance with the principles of the GDPR

Legal basis

Sikt

What is a “legal basis” for processing?

- Processing is lawful only if certain conditions/grounds apply

- Legal bases are found in (GDPR):
  - Article 6 (general categories)
  - Article 9 (special categories)

Sikt

Consent

Consent - Article 6 (a)

Explicit consent - Article 9, 2(a)

Requirements for consent

- Freely given, specific, informed and unambiguous
- Clear affirmative act (opt in)
- The controller must be able to demonstrate that consent has been given
- It should be as easy to withdraw consent as to give it
- Recital 33 opens for broad consent for research purposes
- See articles 4 (11) and 7 in GDPR

Sikt

Public interest

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (e)).

processing is necessary for archiving, scientific or statistical purposes in accordance with Article 89.1 and based on Union or Member State law (Article 9, 2 (j)).

Appropriate Safeguards

(Article 89 (1))

Data must be adequate, relevant and limited to what is necessary – principle of data minimisation

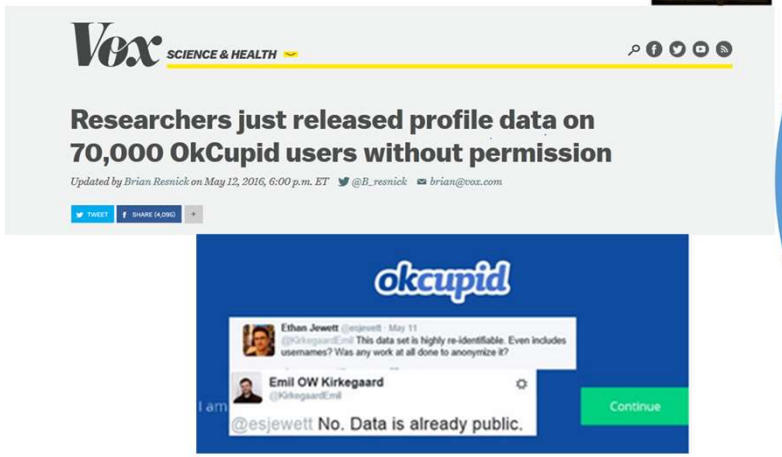
- **Technical measures:**
  - Safe data and safe environments
  - Anonymisation, pseudonymisation and encryption
  - Remote access solutions

- **Organisational measures:**
  - Data Protection Officer involvement
  - Ethical review

Social media data?

processing relates to personal data which are manifestly made public by the data subject (Article 9, 2 (e))

The fine line between private and public



People may operate in public spaces but maintain strong perceptions or expectations of privacy (AoIR 2012).

Sikt

What about Children and Youth?

Conditions applicable to child's consent in relation to *information society services*

Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. [2]

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

- The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.

- Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand

(Recital 58).

GDPR and children and youth

- Children need particular protection because they may be less aware of the risks involved.
- If you process children's personal data you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option.

www. ico.uk.org

Sikt

Children and youth (2)

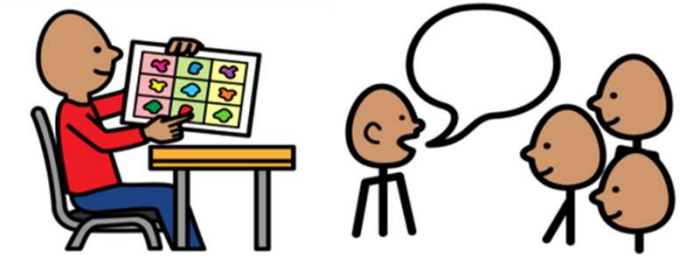
- If you are relying on consent as your lawful basis for processing, you might need to get consent from whoever holds parental responsibility for the child
- You should write clear information letters for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

www. ico.uk.org

Sikt

9. I WANT YOU TO KNOW THERE IS NO RIGHT OR WRONG ANSWERS. EVERYTHING YOU SAY IS IMPORTANT TO ME.

10. AFTER OUR CHAT WE MIGHT GET OTHER HELPERS TO JOIN. WE CAN THEN SHARE THE PHOTOS WE HAVE TAKEN AND TALK ABOUT THEM ALL TOGETHER.



11. WHEN I DO MY SCHOOL PAPER, I WANT TO INCLUDE THE THINGS WE HAVE TALKED ABOUT.

Informing children about their rights as research participants

- https://www.youtube.com/playlist?list=PLYwSkJsQT-91yoTuy9OI6CFodz_M-PNiB

Rights of data subjects

What rights do data subjects have?

What do these rights entail?

- search.creativecommons.org/; future.agenda/CC BY-NC-SA 2.0

Sikt

Rights

- right to be informed
- right of access
- right to rectification / correction of incorrect personal data
- right to erasure / deletion
- right to restrict processing
- right to data portability (a copy)
- right to object to processing
- rights in relation to automated decision making and profiling
- right to lodge a complaint with the supervisory authority

Right to be informed

- Ensures fair and transparent processing
- Must meet requirements for form and content
- Information should be adjusted to the recipient

- See articles 12, 13 and 14

Sikt

Content

- which institution is responsible for the project (the data controller)
- contact details for institution (project leader) and the data protection officer (if applicable)
- the purposes of processing personal data and legal basis for processing
- who will have access to/receive the personal data (e.g. project group, external researchers, data processors)

Content (2)

- if applicable, that personal data will be transferred to a third country or international organisation, and the legal basis for transfer (including which safeguards will protect the data)
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- what rights the data subjects have and how they exercise their rights
- if processing is based on consent: the right to withdraw consent at any time

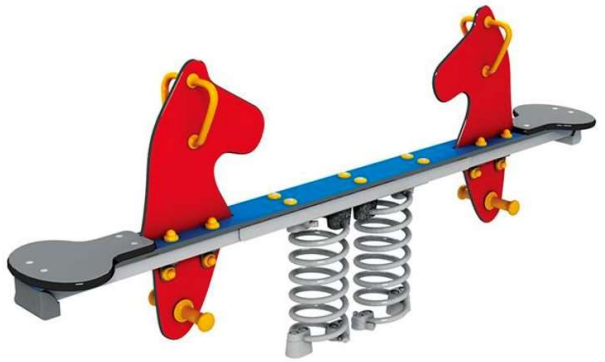
Rights apply so long as the data subject can be identified in the collected data

Exemptions from rights must be justified and must have a legal basis

Sikt

The social benefit vs. risk/disadvantage for data subjects

- Risk to the rights and freedoms of data subjects depends on, i.a.:
  - how sensitive the data is
  - how easy it is to identify individuals
  - the quantity of personal data
  - how securely the data is being stored



Sikt

Data Protection Impact Assessment (DPIA)

- A DPIA is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is likely to result in a high risk to individuals.

EDPB has set 9 criteria:

- Sensitive data or data of a highly personal nature (4)
- Data processed on a large scale(5)
- Data concerning vulnerable data subjects (may include children) (7)

Transfer to third countries

Any dataflow to countries outside of the EU

Sikt

Basis for transfers

- Adequacy decision: Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay , Japan, the United Kingdom and South Korea.
- Appropriate safeguards (standard contractual clauses with supplemental measures)
- Derogations for specific situations

Case - youth

- Research project involving teenagers in high school (15/16 years old)
- Video recordings of classroom situations, focus is on teaching methods
- Data will be stored for 30 years and entered into a data base where data will be shared with other researchers in the future

Questions for discussion:

- Is informed consent or public interest the best legal basis?
- How to collect consent? Can the teenagers' consent on their own or should parents give their consent/be informed?
- What if not the whole class consents to participation?
- What if someone at a later point wishes to withdraw their consent/requires that their data is deleted?
- How to write the information letter in order to open up for future researchers being able to access and use the data in the future?

TIP 3:

Be realistic.

Don’t limit yourself unnecessarily.

Why?

- Based on our experience researchers often underestimate how long time they will need to achieve their research purposes.
- Researchers find data protection legislation challenging **BUT** it is not necessary to delete all your collected data at the end of the project.
- Anonymised data can (and often should) be archived for future research purposes.
- Personal data can also be archived

Sikt

TIP 4:

Be organized and have a system

Why?

When collecting, storing and analysing data don't take anything for granted….

- expect to forget which interviewee is which
- store names (directly identifiable data) separately from other data
- keep your metadata
- prepare for sharing/reuse/archiving

Think about **FAIR** principles in advance. That your future data should be:

- Findable
- Accessible
- Interoperable
- Reusable

Guidelines from your institution

Familiarise yourself with your institution's **information security guidelines**, e.g. whether there are requirements for where data is stored, or which survey provider you should use.

Sikt

Important considerations

1. Will you handle personal data?
2. Will you handle sensitive data?
3. Will your data contain information about third persons?
4. Is some of the data likely to be considered sensitive to the person in question?
5. Might the research lead to unwarrented stigmatisation or discrimination against a group?
6. Do any of the data subjects constitute/represent vulnerable groups (i.e . children, vunerable adults)?
7. What is the legal basis for collecting data?
8. Is it necessary and/or possible to inform the data subjects?
9. Ownership/terms og use
10. How can you make your data FAIR?

- https://seriss.eu/wp-content/uploads/2019/08/SERISS-D6.2.-Guidelines-social-media-data-.pdf
- https://sikt.no/en/information-and-consent

Thank you for listening!

Sikt

Share your experience

1) Have you ever been in contact with data protection officer (DPO)?

1) Have you ever consulted ethical committee at your institute?

COORDINATE

Protect: Different access levels available

OPEN ACCESS

STANDARD ACCESS

ACCESS UNDER SPECIAL CONDITIONS

https://www.adp.fdv.uni-lj.si/eng/uporabi/kako/pravila/

UK Data Service

OPEN DATA

SAFEGUARDED DATA

CONTROLLED DATA (SECURE LAB)

https://ukdataservice.ac.uk/help/access-policy/types-of-data-access/

COORDINATE