

RESEARCH ON PEOPLE

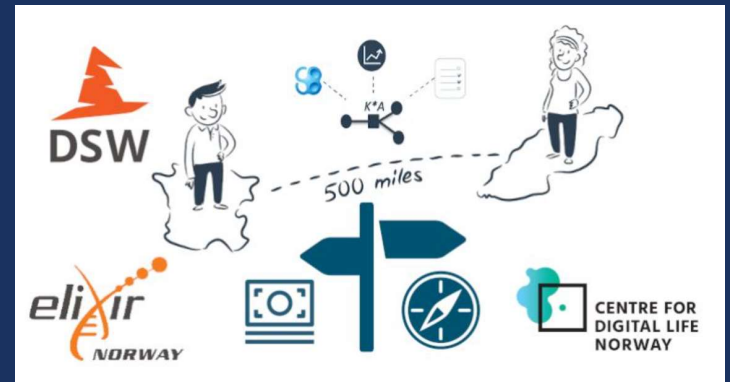
«HOW CAN WE DEVELOP A NATURAL HUNCH FOR GDPR»



1.12.2020

0900 - 1000 GDPR and other legal requirements for research on humans

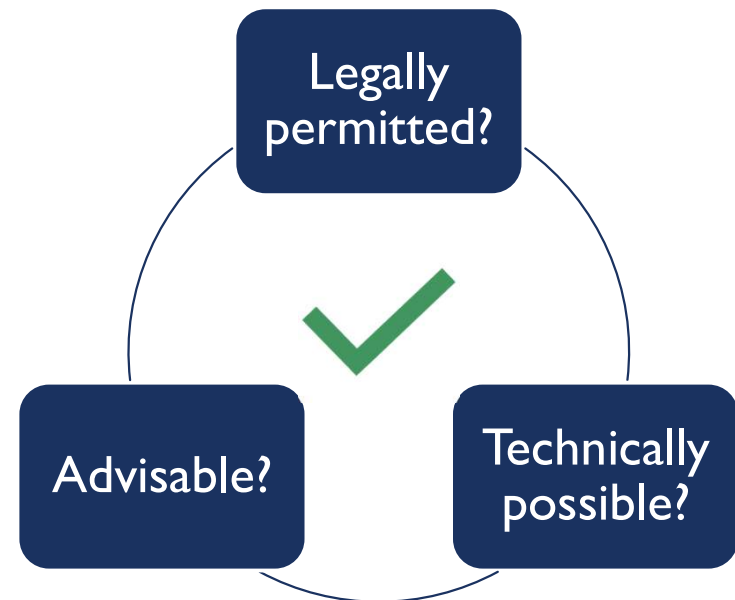
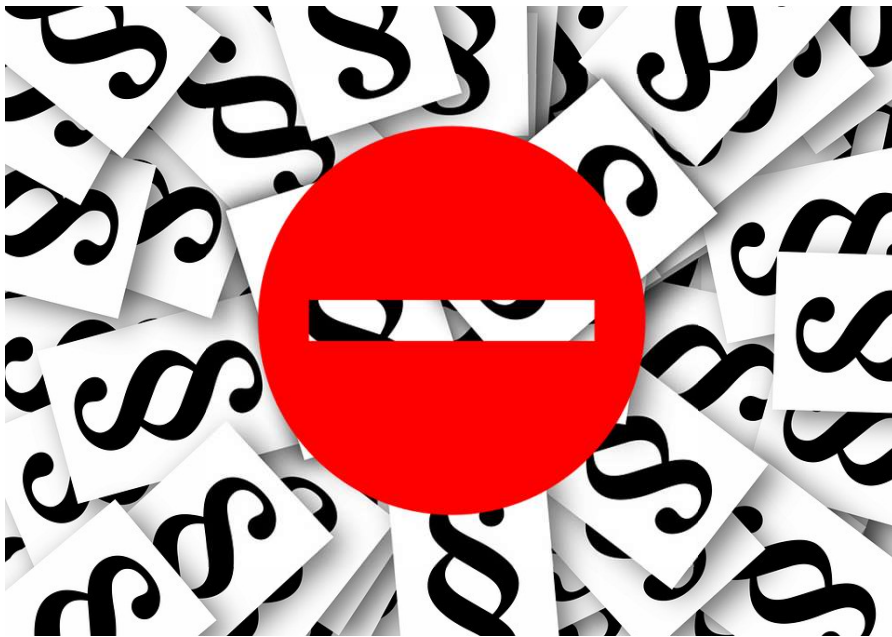
- Health Research Act
- Personal Data Act



GENERAL DATA PROTECTION REGULATION (GDPR)



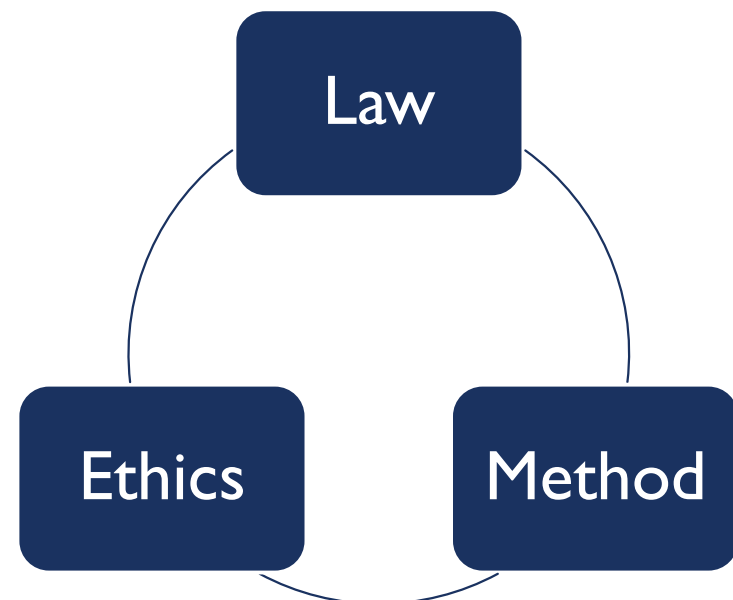
FROM PARAGRAPHS TO «THE HUNCH»



GDPR – WHAT DO WE EXPECT FROM YOU?



- You need to know the meaning of **personal data**
- You need to have a **lawful reason** to process personal data
- Assessments made for the lawfulness of processing and security measures are **documented**
- NTNU needs to have control of all handling of personal data:
 - NTNU must have an independent data protection officer
 - Procedures for internal control and discrepancy processing
 - Fulfill protocol requirements



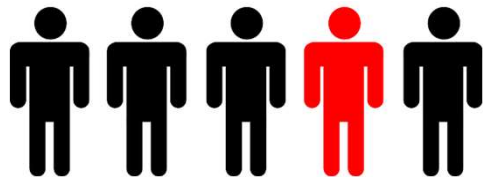
WHAT IS PERSONAL DATA



Any information relating to an identified or identifiable natural person («one who can be identified directly or indirectly»)

For instance

- name, identification number, address, telephone number ++.
- online identifiers, location data, factors specific for physical, physiological, genetic, mental, economic, cultural or social identity ++
- also pictures, sound, video, email, voice, hand writing ++



Special categories of personal data (excerpt)

- Racial or ethnic origin
- Political opinions, religious or philosophical beliefs, trade union memberships
- Sex life or sexual orientation
- Health data
- Criminal convictions and offences
- Genetic and biometric data (fingerprints, dna, voice ++) *with purpose of uniquely identifying a natural person*

LAWFULNESS OF PROCESSING (ARTICLE 6)



What is «processing»?

- Definition (art 4.2):
 - «any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means»
 - E.g. collection, recording, organisation, structuring, adaption or alteration, retrieval, consultation, use +++
- Lawful processing **must** be ensured and documented

“consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

When can we process personal data?

Consent

- given freely and informed. Withdrawable at any time

Necessary lawfulness of processing

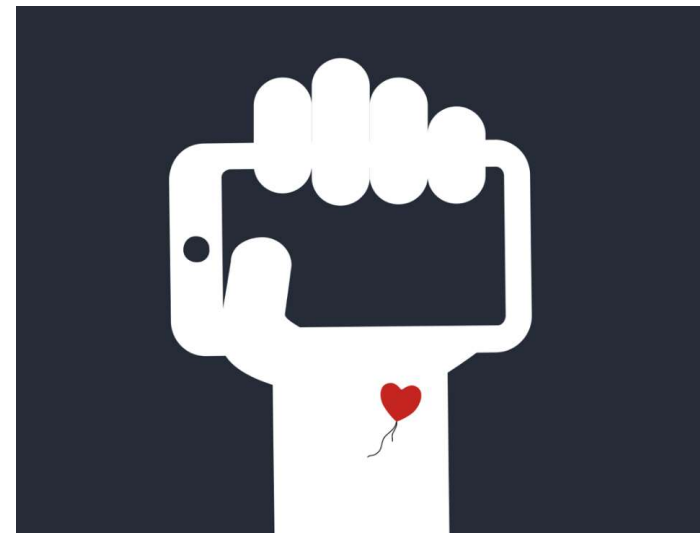
- Fulfill a contract to which the data subject is a party
- Ensure compliance with a legal obligation to which the controller is subject;
- To protect the vital interests of the data subject or of another natural person;
- Ensure performance of a task **carried out in the public interest** or in the exercise of official authority vested in the controller;
- For legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

IT IS MY PERSONAL DATA



The data subject **shall** have the right to

- be informed as to whether or not personal data concerning him or her are being processed
- access to the personal data
- purposes of the processing
- demand correction
- demand deletion (exceptions e.g. **archive** overrules)
- demand limited processing
- protest
- demand data portability
- complain (internally and **externally**)
- receive an answer within 30 days (when he or she asks)
- receive information when unauthorized disclosure of personal data has occurred



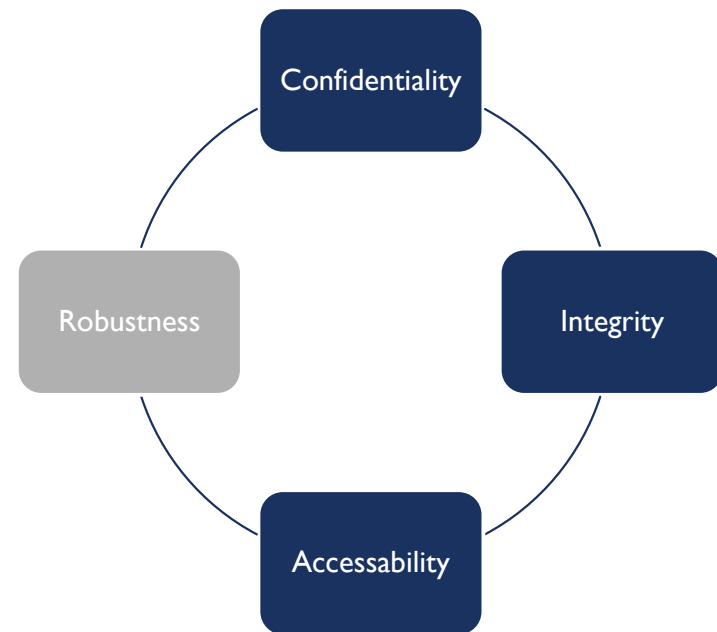
Unknown author, licensed by [CC BY-SA](#)

NB: Many exceptions: archive, statistical purposes, confidentiality, scientific research ++

INFORMATION SECURITY



- Article 5 “Principles”: 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’).
- **As open as possible, as closed as necessary**
- Privacy as a critical value
- Risk assessment and documentation

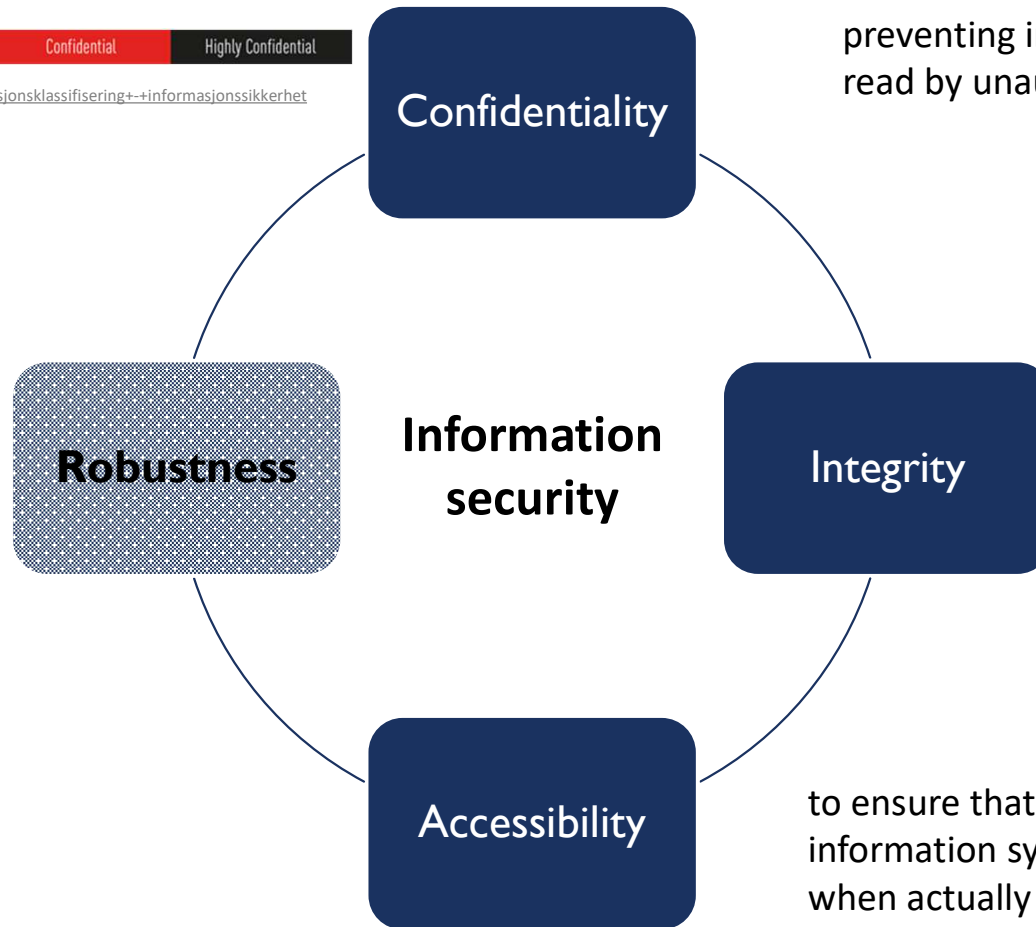


Delete // «Anonymisation is irreversible pseudonymisation»



<https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonsklassifisering+-+informasjonssikkerhet>

Information governance
over time...



preventing information from being read by unauthorized parties.

is the maintenance of, and the assurance of the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data

to ensure that information and information systems are accessible when actually needed.

INFORMATION SECURITY LEVELS



Responsible: NTNU

**NTNU standard
IT-services**

(solutions with institutional
recommendations)

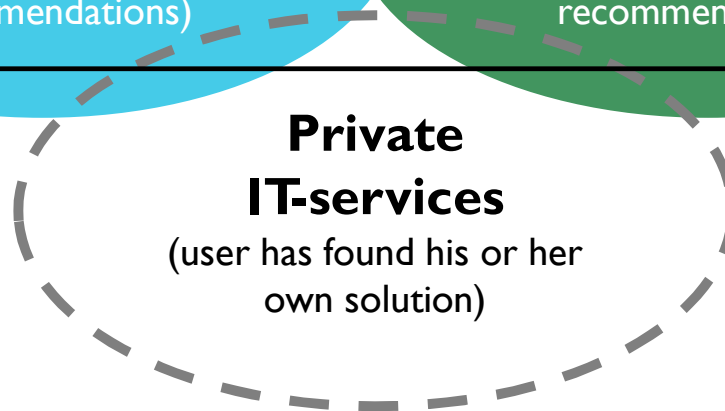
**NTNU local
IT-services**

(solutions with local
recommendations)

**Private
IT-services**

(user has found his or her
own solution)

Responsible: user



If you are processing personal data electronically and it is **not related to medical or health research**, you need to report your project to the Norwegian Centre for Research Data (NSD). This applies to both research and student projects. The same applies if you are manually processing personal data to be entered into a personal data register.

NSD offers advice to students and researchers by telephone, e-mail and **chat**

The Project Manager or supervisor of a student project is responsible for reporting the project to NSD. The project must be reported 30 days before the collection of data is initiated, at the latest. NSD also offers archiving for project data (in Norwegian) when the project is concluded.

NSD DATA PROTECTION SERVICES

<https://nsd.no/>

<https://meldeskjema.nsd.no/test/>

<https://innsida.ntnu.no/wiki/-/wiki/Norsk/Behandle+personopplysninger+i+forskningsprosjekt>

Which personal data will be processed?

[What are personal data?](#)

[What is processing?](#)

Name (also with signature/written consent) [?](#)

☐ Yes ☐ No

National ID number or other personal identification number [?](#)

☐ Yes ☐ No

Date of birth

☐ Yes ☐ No

Address or telephone number

☐ Yes ☐ No

Email address, IP address or other online identifier [?](#)

☐ Yes ☐ No

Photographs or video recordings of people [?](#)

☐ Yes ☐ No

Sound recordings of people [?](#)

☐ Yes ☐ No

GPS data or other geolocation data (electronic communications) [?](#)

☐ Yes ☐ No

Background data that can identify a person [?](#)

☐ Yes ☐ No

Genetic data [?](#)

☐ Yes ☐ No

Biometric data [?](#)

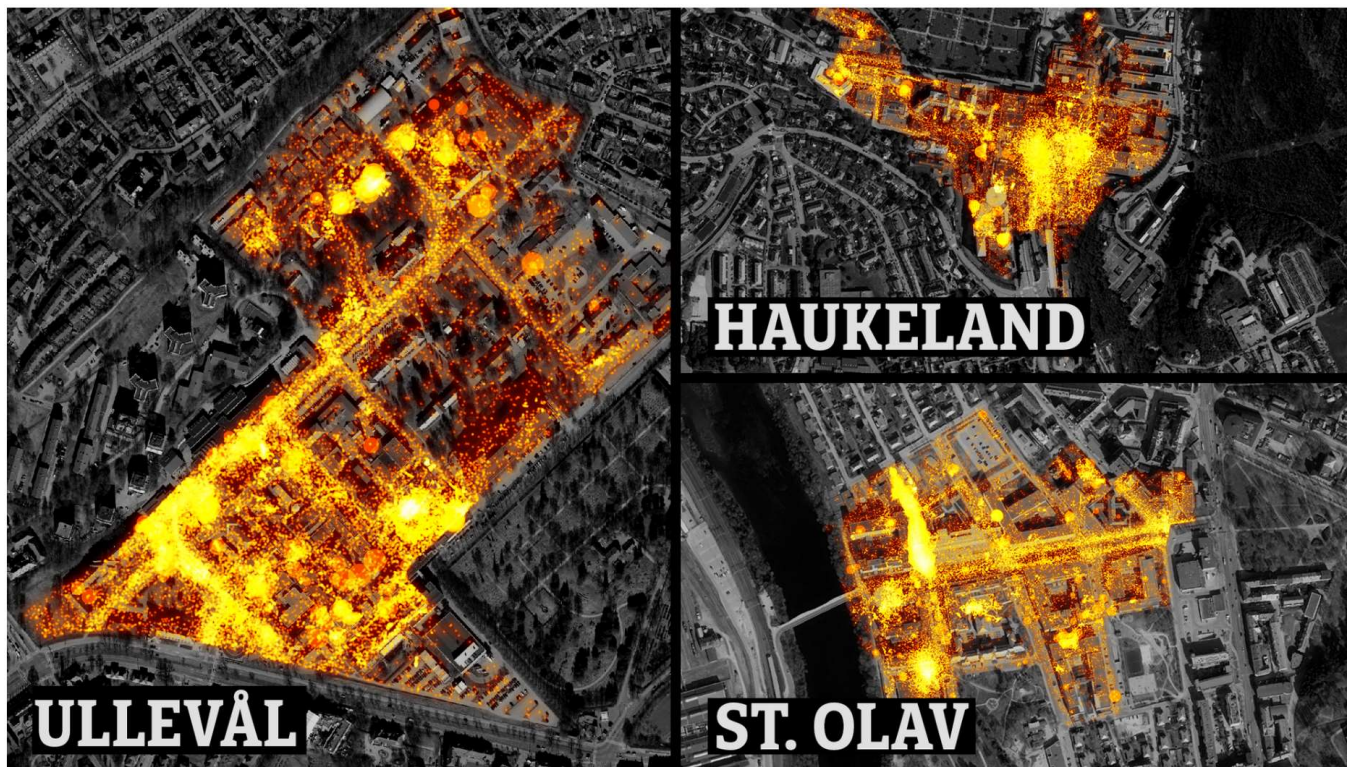
☐ Yes ☐ No

Other data that can identify a person [?](#)

☐ Yes ☐ No

[Continue](#)

WHAT DO WE FEAR?



De gule punktene viser nøyaktig hvor norske mobiler har oppholdt seg på sykehus.

FOTO: HARALD K. JANSSON/NRK

Data from 8300 cellular phones tracked from inside hospitals and crisis centers bought online. cost: 35000 NOK

https://www.nrk.no/norge/mobilsporing_-8300-mobiler-sporet-pa-sykehus-og-krisesentre-1.15008085

Tools:

<https://innsida.ntnu.no/wiki/-/wiki/English/Data+management+plan>

Data management plan

Collect

Use/process

Complete



OPEN
SCIENCE
NTNU



Tools:

<https://innsida.ntnu.no/wiki/-/wiki/English/Data+collection>

Tools:

<https://innsida.ntnu.no/wiki/-/wiki/English/Data+storage+guide>

Tools:

<https://innsida.ntnu.no/wiki/-/wiki/English/Research+data+repository>

WHICH VALUES DO I POSSESS?



Conciouness of which values you actually possess, and what you do with it.

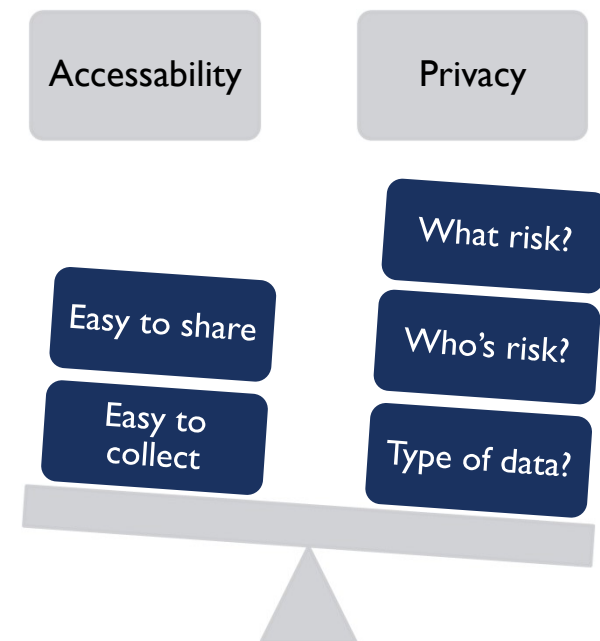
What does these values mean for NTNU? For me as a student/researcher?

Which values do i administer on behalf of someone else? Which risk do I take?

«God folkeskikk» / common decency. The same type of «hunch» as for any other honest and accountable action.

We must build a joint knowledge in the tools we use, and in which context we can use these tools

We must learn to think in a new way



SUMMARY

1. What is affected by GDPR?

All collection of personal data, independent of purpose and context

No difference between different activities (studies/teaching/research)

Research Data / NSD
(m.fl.)

2. What is «personal information»?

Information that makes identification of a physical person possible, on its own or when combined with other data

NB! «Special category data»

Research Data / NSD

3. How should I collect data?

All data collection is «data collection»

What kind of data are you planning to collect?

Data collection guide

4. Where should I save my data?

ENOUGH security for your data – consider the risk

Rule of thumb: use NTNUs internal data storage

Storage guide

5. What should I do with the data after completing a project?

Do what you promised

Deleting and anonymisation must be IRREVERSIBLE

Open Science: As open as possible, as closed as necessary

WHO CAN HELP ME?

DEPARTMENT ADMINISTRATION
LOCAL TEACHING SUPPORT

EDUCATION



RESEARCH



NSD DATA PROTECTION SERVICES

<https://nsd.no/>

**Research
Data @NTNU**

- <https://innsida.ntnu.no/researchdata>
- research-data@ntnu.no