



Data classification

13.10.2023

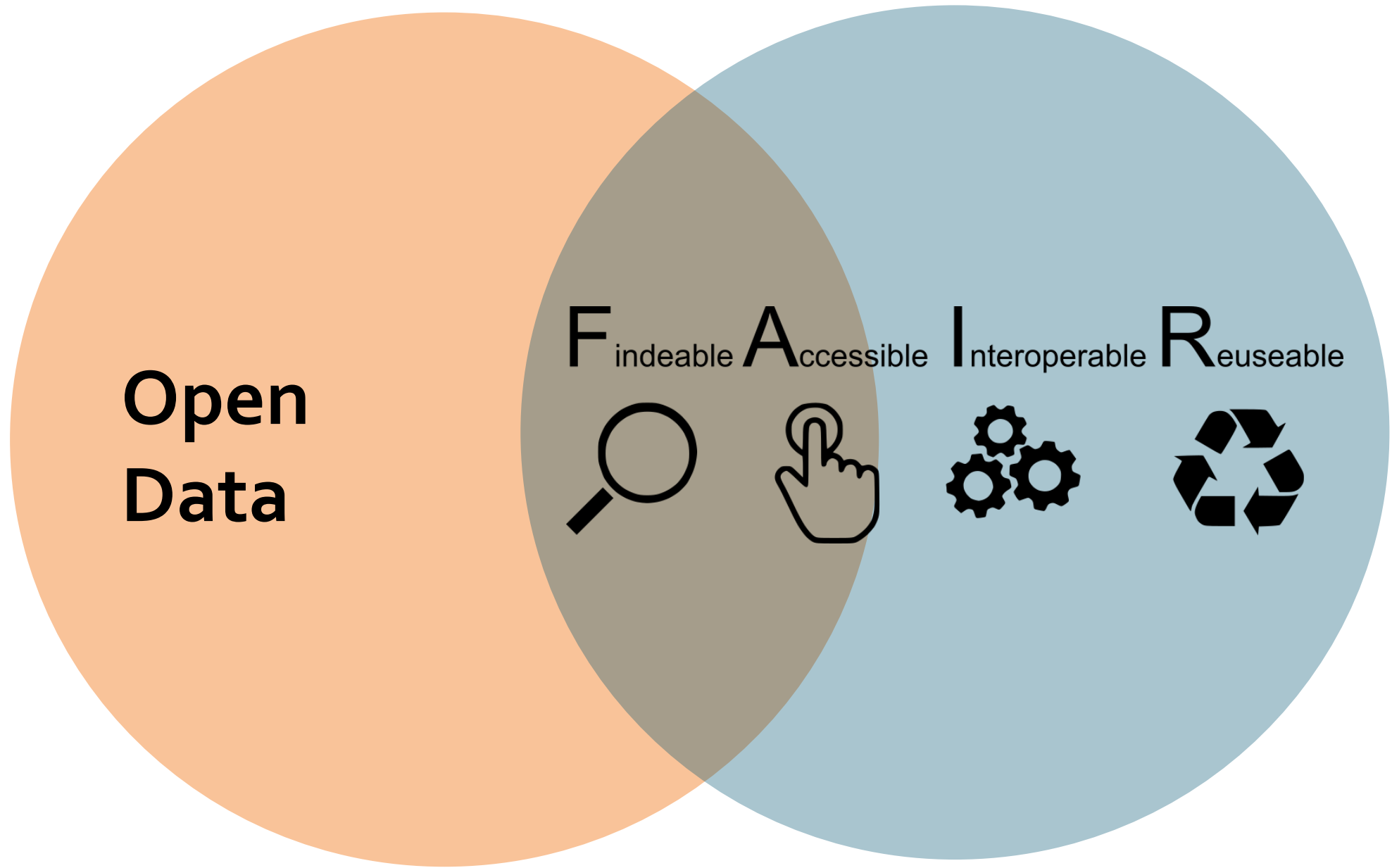


Illimar Rekand (he/him)
Data steward
University of Bergen
ELIXIR Norway

Some slides adapted from Nazeefa Fatima, 2022 under [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)

Disclaimer

This is not legal advice



“As open as possible - as closed as necessary”

Sensitive data:

“Sensitive data is data that must be protected against unwanted disclosure.

Access to sensitive data should be safeguarded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary consideration”



What is personal data? Examples:



A name and surname



A home address



An email address such as
name.surname@company.com;



Location data



An Internet Protocol (IP) address



A cookie



Data held by a hospital or doctor, which could be a
symbol that uniquely identifies a person.



The following personal data is considered 'sensitive' and is subject to specific processing conditions:

- **personal data** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- **trade-union membership**;
- genetic data, biometric data processed solely to **identify a human being**;
- **health-related** data;
- data concerning a person's **sex life or sexual orientation**.

What defines genetic data?



Genetic data is defined as: “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person.” - GDPR article 4(13)



Always both: Personal identifier and sensitive information!

Further reading - what personal data is considered sensitive?:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Take-home message 1:

If you are dealing with data that comes from/relates to people in one form or another....

... you are probably dealing with sensitive data

Important Relevant Legislations

Personal Data Act

Regulations on the processing of personal data

General Data Protection Regulation (GDPR)

The GDPR is an EU Regulation that applies directly to Norway, as a member of the EEA.





GDPR: General Data Protection Regulation



Protection of Personal Data



Privacy by Design



Data Protection Impact Assessment (DPIA)



Processing of Personal Data



Technical and organisational measure to secure data



Records of Processing Activities



Access rights, Right to be forgotten, Right on Information



Fines: Up to 20 million Euros (<4 % of total global turnover preceding fiscal year)



What does GDPR say about:

Data subjects, processing, controller, and processors

- **Data subject:**
“the natural person information relates to.”- GDPR article 4(1)
- **Data Processing:**
“any operation or set of operations which is performed on personal data or on sets of personal data.” - GDPR article 4(2)
- **Data Controller:** determines the purposes and means of the processing of personal data
- **Data Processor:** processes personal data on behalf of the controller

Conditions to store/process personal (sensitive) data

- Lawful and transparent manner (**'lawfulness, fairness and transparency'**)
- Specific purposes (**'purpose limitation'**)
- Only the personal data that is necessary to fulfil that purpose (**'data minimisation'**)
- Stored for no longer than necessary (**'storage limitation'**)
- **Data Accuracy**
- Technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology (**'integrity and confidentiality'**)
- **Accountability** → Immediate reporting of incidents

Criteria to store/process personal (sensitive) data



Explicit consent from participant

Health Research Act



- The data is processed for **archiving, scientific or historical research** purposes or statistical purposes on the basis of EU or national law.
- “Tasks carried out in the public interest” - Article 6, GDPR
- “It is not always possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection” - GDPR, Recital 33

Further readings:

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en
- https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_4#KAPITTEL_4



Criteria to store/process personal (sensitive) data



Explicit consent from participant

Health Research Act



If you are using consent as your legal basis:

**Make sure your consent form (& REK* approval)
allows controlled access deposition (e.g. to EGA**)
...before you start!**

* REK: Regional Committees for Medical and Health Research Ethics

** EGA: European Genome Archive

Further readings:

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en
- https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_4#KAPITTEL_4

Important Relevant Legislations

Research Ethics Act

Health Research Act

Health Registry Act

Biotechnology Act

Archive Act

Patents Act

Copyrights Act



- Health Register Act: <https://lovdata.no/dokument/NL/lov/2014-06-20-43>
- Biotechnology Act: <https://lovdata.no/dokument/NL/lov/2003-12-05-100>
- Archives Act: <https://lovdata.no/dokument/NL/lov/1992-12-04-126>
- Patents Act: <https://lovdata.no/dokument/LTI/lov/2019-06-21-49>
- Copyright Act: <https://lovdata.no/dokument/NL/lov/2018-06-15-40>



Personal Data Act & Personal Data Regulations

National Implementation of GDPR



Consent from participants (13 years and older)



Exceptions for archival, public interest, and scientific reasons



Authorities: Privacy Ombudsman, Privacy Committees,
Data Inspectorates (datatilsynet)

More information at:

- Regulations on the processing of personal data: <https://lovdata.no/dokument/SF/forskrift/2018-06-15-876>
- Transitional rules on the processing of personal data: <https://lovdata.no/dokument/SF/forskrift/2018-06-15-877>
- Personal Data Act: <https://lovdata.no/dokument/NL/lov/2018-06-15-38>



Research Ethics



- Withhold-, mislead about-, or selectively/secretly dispose of undesired results



- Improper allocation of authorship etc.
- Concealment of scientific efforts and / or scientific achievements.



- Destruction of research data / material to prevent investigations of misconduct

Research Ethics Act: _____

<https://lovdata.no/dokument/NL/lov/2017-04-28-23>



Health Research Act



Prior approval for health research



Consent from participants



Data access rights for participants



Biobank Regulations



Maximum data storage time for non-archived data
(Default: 5 years after end of project – exemptions: approval)



Regional Committees for Medical and Health Research Ethics (REK)



Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)

Dato	FOR-1972-03-17-3352
Departement	Justis- og beredskapsdepartementet
Publisert	I 1972 369
Ikraftredelse	01.07.1972
Sist endret	FOR-2019-02-08-72

➔ Gå til opprinnelig kunngjort versjon

Lov om medisinsk og helsefaglig forskning (helseforskningsloven)

Dato	LOV-2008-06-20-44
Departement	Helse- og omsorgsdepartementet
Sist endret	LOV-2020-12-04-133 fra 01.06.2021
Ikraftredelse	01.07.2009
Kunngjort	20.06.2008 kl. 14.40
Rettet	02.07.2021 (faglige fotnoter fjernet, UU-tilpasset)
Korttittel	Helseforskningsloven – hforsknl

Se også lov 28 apr 2017 nr. 23. Sml. lov 21 feb 2003 nr. 12.

Kapittel 1. Lovens formål og virkeområde

§ 1. Formål

Lovens formål er å fremme god og etisk forsvarlig medisinsk og helsefaglig forskning.

§ 2. Lovens saklige virkeområde

Loven gjelder for medisinsk og helsefaglig forskning på mennesker, humant biologisk materiale eller helseopplysninger. Slik forskning omfatter også pilotstudier og utprøvende behandling.

For behandling av helseopplysninger gjelder personvernforordningen og personopplysningsloven med forskrifter, i den utstrekning ikke annet følger av denne loven. For opplysninger som er taushetsbelagte etter helsepersonelloven § 21, og for opplysninger om avdøde personer gjelder bestemmelsene i loven her om behandling av helseopplysninger så langt de passer. Loven gjelder ikke for etablering av helseregistre.

For klinisk utprøving av legemidler på mennesker gjelder legemiddeloven § 3 med forskrifter. For klinisk utprøving av medisinsk utstyr gjelder lov om medisinsk utstyr med forskrifter. Loven her gjelder utfyllende så langt den passer.

- Norwegian law dictates how graded information needs to be handled
- Norwegian law dictates how medical research can be conducted



Fairness and Transparency

- Fairness: Not taking advantage of your position as a research institution, and not taking advantage of your position in relation to the data subjects
- Transparency: Your data subjects shall be informed of what you do with their personal data, and of how to exercise their rights
- Provision of the required information in a clear and plain language

Further reading:

<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing->

[data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-)

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1888-1-1>

https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_8#KAPITTEL_8

Data Minimisation

- The amount of personal data shall be limited to that necessary to achieve the purpose of data processing
- Obligation to avoid collecting, storing or in any other way processing personal data that is not strictly necessary, even if it may be “nice to have”

Further reading:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1888-1-1>
https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_8#KAPITTEL_8

Data Accuracy

- Important not only in consideration of the data subjects but also for your research
- Obligation to rectify or delete inaccurate personal data
- Your data subject can ask for deletion of the data at any time

Further reading:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1888-1-1>
https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_8#KAPITTEL_8

Storage Limitation

- Personal data shall not be stored for longer than necessary to fulfil the purpose
- Once the purpose has been achieved, the data shall in principle be deleted or made anonymous
- REK usually sets requirements for storage beyond the project period for reasons of verifiability - you may need to include this in your application!
- Processing personal data for the purpose of verifiability is legitimate
- Personal data may be stored for longer periods so far as the personal data is processed solely for scientific, historical, and/or statistical research

Further reading:

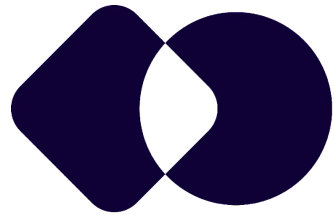
<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing->

[data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en)

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1888-1-1>

https://lovdata.no/dokument/NL/lov/2008-06-20-44/KAPITTEL_8#KAPITTEL_8

Responsible Authorities



Sikt
Kunnskapssektorens
tjenesteleverandør



Datatilsynet



Helsedirektoratet



REK

REGIONAL COMMITTEES FOR MEDICAL AND HEALTH RESEARCH ETHICS



De nasjonale

**FORSKNINGSETISKE
KOMITEENE**



**Statens
legemiddelverk**

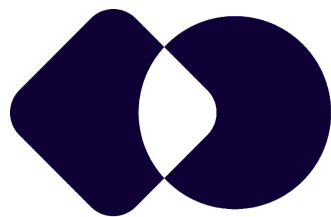


Data Privacy Assessments

Since 2020:

Sikt carries out privacy assessments on behalf of Norwegian universities. Processing personal data in project → Apply to Sikt

Minimum 30 days before data collection



Sikt
Kunnskapssektorens
tjenesteleverandør

<https://sikt.no/en/notification-form-personal-data>

What constitutes a breach of personal data protection?



Breach in (either intentionally or unintentionally):

- **Confidentiality**
Information has been leaked
- **Integrity**
Information has been changed
- **Availability**
Access/Denial, access/deletion

If suspected breach:
Duty to report!

How and where to report?

Hva er et brudd på personopplysningssikkerheten?

Et brudd på personopplysningssikkerheten (*avvik*) er i *personvernforordningen* definert som utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.



[https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hva-er-et-brudd-pa-personopplysningssikkerheten/#:~:text=Et%20brudd%20p%C3%A5%20personopplysningssikkerheten%20\(avvik,eller%20p%C3%A5%20annen%20m%C3%A5te%20behandlet](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hva-er-et-brudd-pa-personopplysningssikkerheten/#:~:text=Et%20brudd%20p%C3%A5%20personopplysningssikkerheten%20(avvik,eller%20p%C3%A5%20annen%20m%C3%A5te%20behandlet)

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/meld-avvik-til-datatilsynet/>

REK

- Health research based on personal data needs approval from Regional Etisk Komité (REK) before the research project starts
- Inquiries are sent to the relevant region
- Deadlines throughout the year



Other reasons data can be considered sensitive:

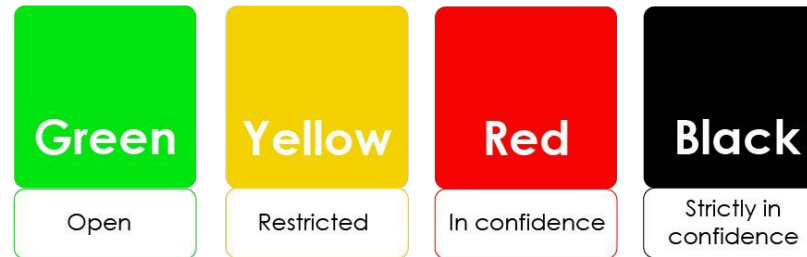
- Intellectual property rights (IPR):
Patentability, trade secrets, investigations
- Strategy documents
- Biological data: Endangered species (location data)

Subsets of data classification

Integrity and Confidentiality

- Personal data must be processed in a manner that ensures:
- appropriate security of the personal data,
 - protect personal data against unauthorized access,
 - unlawful processing,
 - accidental loss, distribution, amendment or damage

Follow institutional guidelines



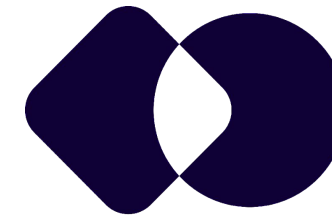
- Pseudonymisation
- ◆ Dedicated data analysis platforms

Image Source: <https://uio.no/english/for-employees/support/research/funding/units/hf/imv/data-ethics/colors.htm>

More about TSD: <https://www.uio.no/english/services/it/research/sensitive-data/>

Sikt –

Norwegian Agency for Shared Services in Education and Research



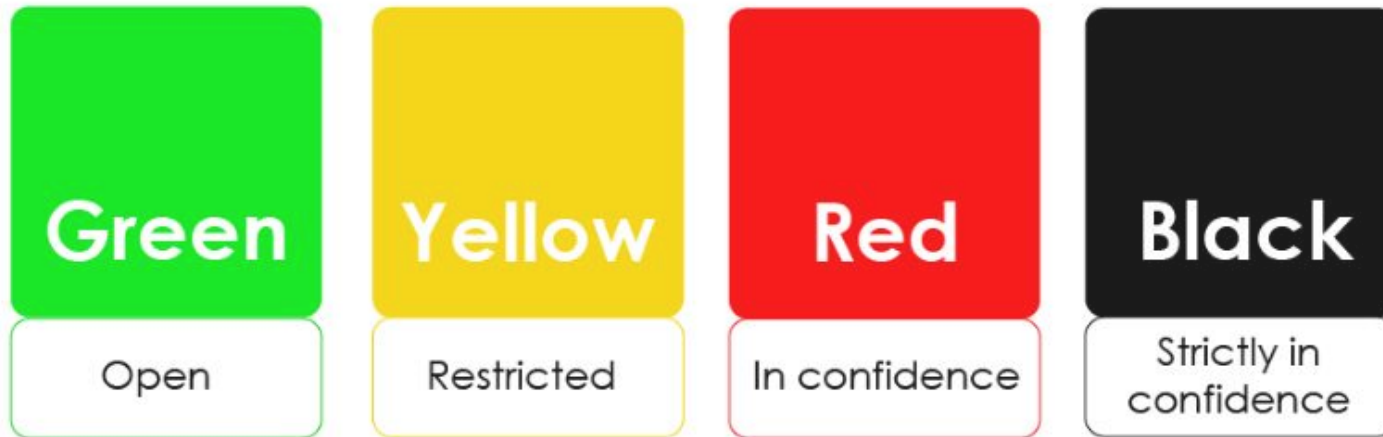
Sikt
Kunnskapssektorens
tjenesteleverandør

- General guidelines for data classification
- Archives sensitive data of “people and society” with different levels of access

Konfidensialitet	Integritet	Tilgjengelighet
Lav Åpen	Lav Uoffisiell	Lav Unnværlig
Middels Beskyttet	Middels Offisiell	Middels Forventet
Høy Fortrolig	Høy Forvaltet	Høy Vesentlig
Kritisk Strengt fortrolig	Svært høy Uerstattelig	Svært høy Uunnværlig
SKJERMINGSVERDIG ETTER SIKKERHET SLOVENS BESTEMMELSER Informasjonen kan også samtidig ha beskyttelsesbehov av andre forhold		
Konfidensialitet	Integritet	Tilgjengelighet
BEGRENSET (lavgradert)		
KONFIDENSIELL		
HEMMELIG		
STRENGT HEMMELIG		

Dersom sikkerhetsbrudd kan ha betydning for nasjonale sikkerhetsinteresser, utløses beskyttelseskrav fra sikkerhetsloven. Informasjonen vil da omtales som *skjermingsverdlig*, og skal ikke lenger klassifiseres etter sektorstandard for informasjonssikkerhet.

University of Oslo - guidelines for data classification



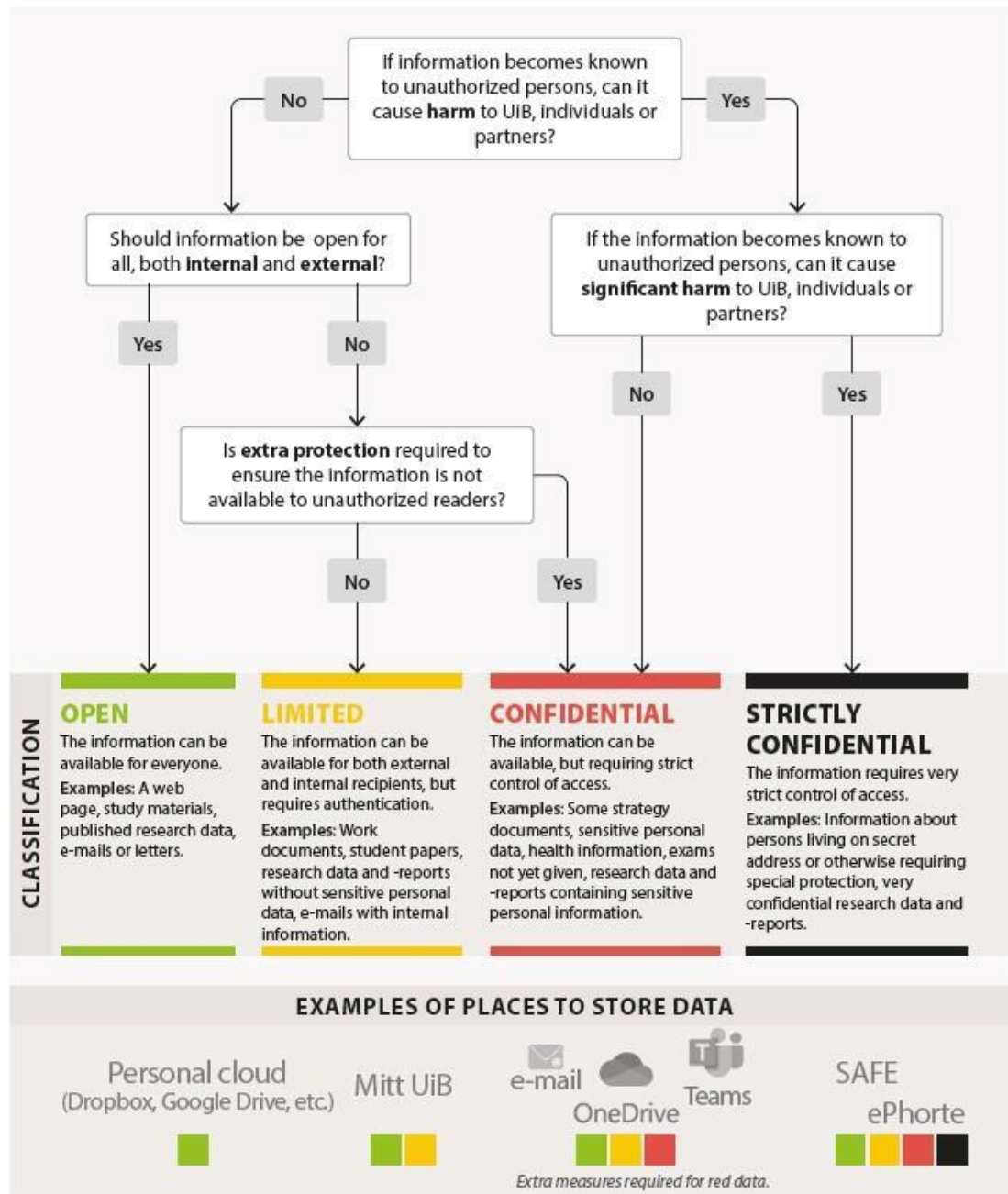
many types of
personal data

special category
(personal sensitive)
data

large amounts of
special category
data

WHAT DATA CAN BE STORED WHERE?

You are responsible for classifying and securing information!



University of Bergen guidelines for data classification

SAFE is the recommended solution for handling sensitive data





Read more about:

- [Classification of information \(Norwegian\)](#)
- [Classification of files and documents](#)

Classification of personal data

Research data is usually classified as internal (yellow) or confidential (red), and this also applies to research data containing personal data. Personal data is information and assessments that can be related to individual persons, either directly or indirectly. Examples include names, ID-numbers, e-mail, IP-addresses, photos, videos, interview recordings and transcribed interviews.

Storage services and collaboration platforms

Storage services and collaboration platforms refer to cloud services or servers at NTNU. Click on the different solutions for more information.

	Public	Internal	Confidential	Highly confidential
Personal cloud storage (dropbox, google drive ++)	OK	NO	NO	NO
NTNU Personal home directory («M:-drive»)	OK	OK	OK	OK (1)
NTNU Shared directory (T:-drive, group, project, etc.)	OK	OK	NO	NO
NTNU-administered Dropbox (contact Orakel)	OK	OK	NO	NO
NTNU-Box	OK	OK	NO	NO
Office 365 (SharePoint, Teams, Onedrive)	OK	OK	OK(1)	NO
NTNU NICE-1 - Storage solution with added security	OK	OK	OK	OK (1)
HUNT Cloud	OK	OK	OK	OK (2)
UiO TSD	OK	OK	OK	OK
NIRD (tidligere Norstore, driftes av Uninett Sigma2)	OK	OK	NO	NO

(1) Data must be encrypted. [Read more on how to encrypt O365 files using AIP here](#) or [how to encrypt other files with 7-Zip](#)

(2) Risk level is assessed on individual basis, see the [HUNT information page for more information](#).

<https://i.ntnu.no/wiki/-/wiki/English/Data+storage+guide#:~:text=Research%20data%20is%20usually%20classified,persons%2C%20either%20directly%20or%20indirectly.>

NTNU - guidelines for data classification



Norwegian University of
Science and Technology

Institutional policies on research data

We provide here a non-exhaustive list of research institutions with Data Management Policies in Norway:

- Norwegian University of Life Sciences (NMBU)
- Norwegian University of Science and Technology (NTNU)
- University of Bergen (UiB)
- University of Oslo (UiO)
- The Arctic University of Norway (UiT)
- University of Stavanger
- University of Agder
- Nord University
- Inland Norway University of Applied Sciences
- Svalbard Integrated Arctic Earth Observing System, SIOS

Institutional storage guidelines

Most universities in Norway classify data into four categories, depending on access requirements. These categories are based on recommendations from UNIT.

- **Open (Green):** Information can be available to everyone, without special access rights.
- **Restricted (Yellow):** Information must have some protections if access by unauthorised persons could harm the institution or collaborators in some way. The information can be available both internally and externally with controlled access rights.
- **Confidential (Red):** Information must have strict access rights if unauthorised access would cause damage to public interests, individuals, the institution, or collaborators.
- **Strictly confidential (Black):** Information must have the strictest access rights if unauthorised access could cause significant damage (for example, highly confidential research or confidential addresses).

Details and provided solutions vary according to each institution:

- Norwegian University of Life Sciences (NMBU) - login
- Norwegian University of Science and Technology (NTNU)
- University of Bergen (UiB)
- University of Oslo (UiO)
- The Arctic University of Norway (UiT)

RDMkit has an overview of the different institutional guidelines



RDM resources/policies in Norway
https://rdmkit.elixir-europe.org/no_resources#institutional-policies-on-research-data

Does my data need require protection?



- **personal data** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- **trade-union membership**;
- genetic data, biometric data processed solely to **identify a human being**;
- **health-related data**;
- data concerning a person's **sex life or sexual orientation**

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Data
↓
Is the data from people?

Yes

No

Do you wish to use the data as a basis for a patent?

No

Probably needs special protection

Yes

Does the data fall under the European Commission definition of personal data?

No

Probably no special protection

Yes

Does it fall under special category data?

Yes

No

Probably needs special protection

Probably does not need special protection

Would it be harmful for you, the institution you are working for or anyone else if the data was available for anyone else?

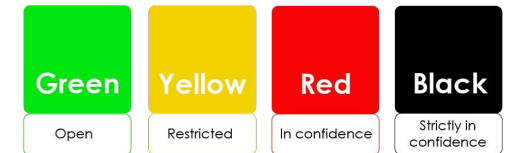
Yes

No

Probably needs special protection

Probably does not need special protection

If sensitive; how should it be classified?



Not sensitive

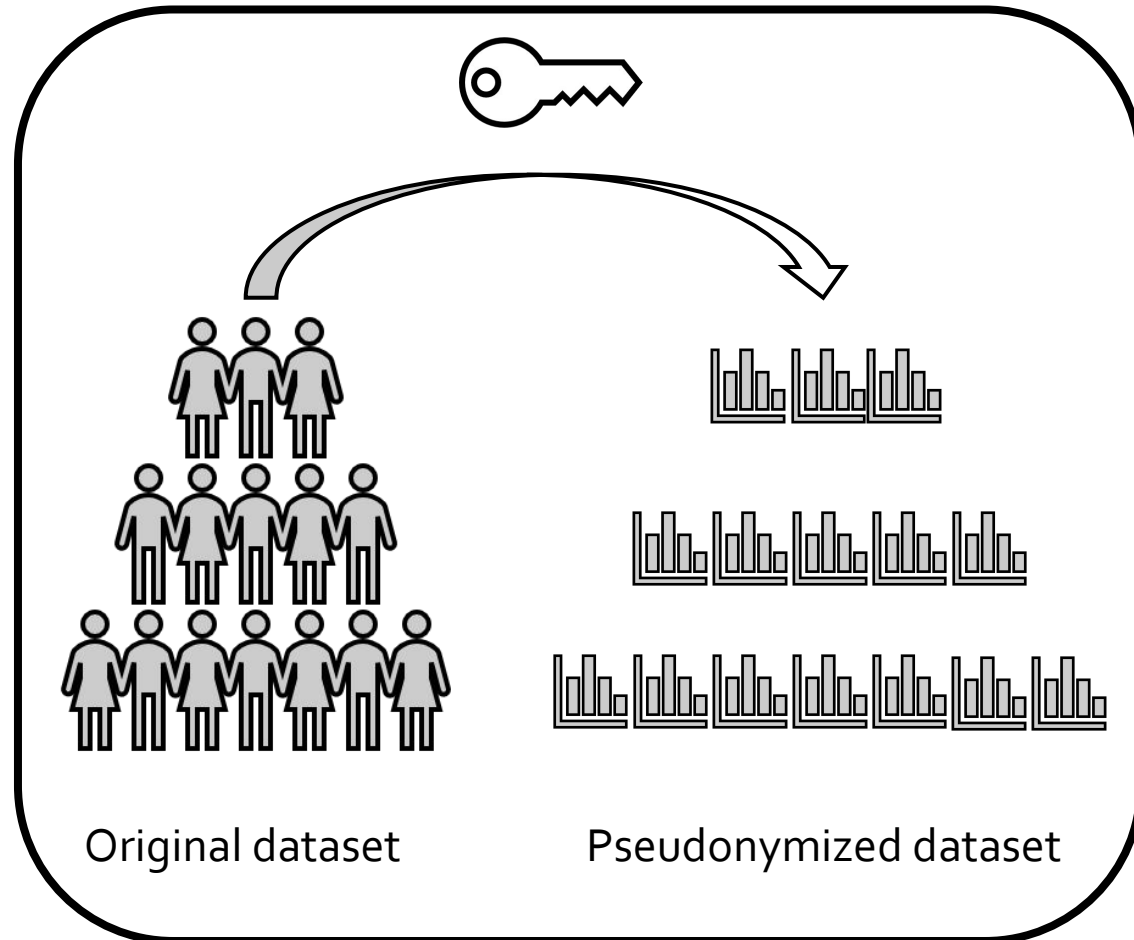
Take-home message 2:

Familiarize yourself with how your institution deals with data classification

How to deal with sensitive data:

- special attention should be given to collecting, processing, handling and storing data throughout the research process
- Address in a DMP how the above will be dealt with

Data Pseudonymisation



© Tomas Castelazo,
tomascastelazo.com / [Wikimedia Commons](#) / [CC BY-SA 4.0](#)

Data 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, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person” - GDPR article 4(13)

→ De-identified and not back traceable for the researcher without the identifier

!! Pseudonymised data is still personal data!

Anonymous Data

→ Anonymous data cannot in any way be used to identify individuals in a data material, either:

- ◆ directly by name or personal identification number
- ◆ indirectly by additional information

! Not possible for many data types, such as genetic data !

Is it still possible to distinguish one individual person in a data set?

Is it still possible to link together various data sets associated with one and the same person?

Is it still possible to deduce information associated with an individual person?



Datatilsynet

Addition of noise	Yes	Probably not	Probably not
Substitution	Yes	Yes	Probably not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	Probably not
Differential privacy	Perhaps/probably not	Probably not	Probably not
Hashing (tokenisation)	Yes	Yes	Probably not
Pseudonymisation	Yes	Yes	Yes

- The Norwegian Data Protection Agency (Datatilsynet) has created some recommendations for secure anonymization
- “At an early stage, the data controller must decide whether the personal data to be processed should be anonymised, de-identified or left identifiable.”

Take-home message 3:

Data pseudonymization (aka. deidentification)

≠

Anonymization



International Data Transfers

Key relevance in scientific research

Countries outside the EU/EEA (“Third countries”)

Transfer mechanism pursuant to GDPR chapter 5

Adequacy Decision

Most common: Standard Contractual Clauses (SCCs) adopted by the European Commission (EC)

Additional safeguards - e.g. Pseudonymization

EC has recognized:

Andorra, Argentina,
Canada, Faroe Islands,
Guernsey, Israel, Isle of
Man, Japan, Jersey,
New Zealand, Switzerland,
Uruguay, and the UK



Exchange of personal data & biological material (for research) in any direction requires special and careful additional consideration!

Further reading:

- eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4319-1-1
- ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en
- gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk

Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid

Retningslinjene gir en oversikt over lover og andre føringer som norsk kunnskapssektor må overholde, og peker på sentrale vurderinger og fremgangsmåter for fagmiljøer og for institusjonsledelse og administrasjon. Retningslinjene tilbyr verktøy for å håndtere risikoer og styrke sikkerheten i internasjonalt samarbeid.

› Internasjonalt forsknings- og innovasjonssamarbeid

Her finner du ressurser knyttet til forskningssamarbeid, åpen forskning og deling, og avtaler om forskningssamarbeid.

› Risiko- og sikkerhetsstyring ved kunnskapsinstitusjonen

Her finner du ressurser knyttet til sikkerhetsstyring, rekruttering og ansettelse, og ivaretagelse av ansatte, studenter og gjesteforskere.

› Eksportkontroll, forhåndstillatelse og oppholdstillatelse

Her finner du en oversikt over føringer i eksportkontrollforskriften og internasjonale sanksjoner, ansvaret kunnskapssektoren har på området og anbefalte vurderinger for institusjonsledelse og fagmiljø.

Guidelines for sharing data across borders



› Internasjonalt høyere utdanningssamarbeid

Her finner du en oversikt over kjente utfordringer i internasjonalt samarbeid om høyere utdanning og hva som bør kartlegges med hensyn til samarbeidsland og partnerinstitusjon.

› Akademiske verdier og forskningsetikk

Her finner du ressurser knyttet til akademisk frihet, åpen forskning og forskningsetikk.

› Informasjonssikkerhet og personvern

Her finner du en oversikt over lovverk og verktøy knyttet til utfordringer og ansvar innenfor informasjonssikkerhet og personvern.

Eksportkontroll, forhåndstillatelse og oppholdstillatelse

Her finner du en oversikt over føringer i eksportkontrollforskriften og internasjonale sanksjoner med hensyn til viktige definisjoner og avgrensinger, ansvar, informasjonsressurser og verktøy, samt vurderinger for institusjonsledelse og fagmiljø.

Sist oppdatert : 28. september 2023

På denne siden

- › Hva er internasjonale sanksjoner?
- › Hva er eksportkontroll for kunnskapsoverføring?
- › Hva er formålet med eksportforskriften?
- › Hvilke myndighetsorgan har ansvar for eksportkontroll
- › Forhåndstillatelse for kunnskapsoverføring
- › Oppholdstillatelse for utenlandske forskere og studenter
- › Hvordan søker jeg om forhåndstillatelse for kunnskapsoverføring?
- › Hvilket ansvar har kunnskapsinstitusjonene?
- › Forslag til vurderinger og fremgangsmåter for institusjonens ledelse og administrasjon
- › Forslag til vurderinger og fremgangsmåter for fagmiljø
- › Ressurser og verktøy for etterlevelse av eksportkontroll for kunnskapsoverføring



<https://www.openaire.eu/>


OpenAIRE is a Non-Profit Partnership of 50 organisations, established in 2018 as a legal entity, *OpenAIRE A.M.K.E.*, to ensure a permanent open scholarly communication infrastructure to support European research.

VAT: EL997032008, GEMI: 147492701000

[View Governance →](#)

OpenAIRE is a socio-technical infrastructure for Open Scholarly Communication in Europe.

- Supports Open Science policy alignment and infrastructure convergence at national level via an active network of experts, the **National Open Access Desks**.
- Operates services that connect data sources (**interoperability**) via the [OpenAIRE Guidelines](#) and [PROVIDE](#)), links them together by creating a **global Scholarly Communication Knowledge Graph**, the [OpenAIRE Research Graph](#), supports policy **compliance** and **monitoring**, and provides **value-added services** to enable researchers to publish, share, manage, and discover research.
- Offers **training** (guides, courses, webinars) for upskilling all R&I actors to practice Open Science.

Introducing OpenAIRE in 3 mins 

Questions?

support@elixir.no

Email: Illimar.rekand@uib.no

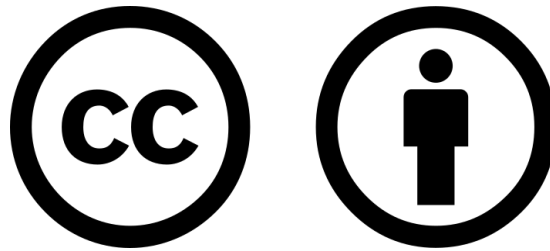
Twitter/X: @illimar

Thank you!

 elixir-norway.org

 @elixirnorway

 support@elixir.no



**Except where otherwise noted, this work is licensed under a
Creative Commons Attribution 4.0 International License**

<https://creativecommons.org/licenses/by/4.0/>



Data Classification © 2023 by Elixir Norway is licensed under CC BY-SA 4.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/>