Retningslinjer for klassifisering og lagring av data og informasjon

Juni/2025 - Ekstern versjon

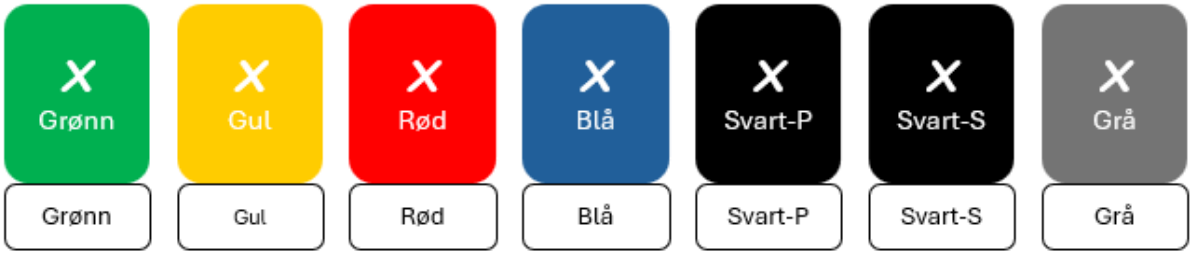
Formål og omfang

Klassifisering av data er nødvendig for å sikre konfidensialitet, integritet og tilgjengelighet til data og informasjon. Retningslinjene gjelder for all data og informasjon som NORCE behandler og lagrer.

Med behandling og lagring av data og informasjon, menes alle data, filer, informasjon og dokumenter som blir opprettet, behandlet og lagret av NORCE, og som vi derfor må sikre en ansvarlig behandling og lagring av. Eksempler er alle administrative data og prosjektdata som Word og Excel dokumenter, e-post og alle forskningsdata.

Retningslinjene er basert på en felles standard i universitets- og høyskolesektoren.

Våre dataklasser:



IT-tjenester: IT-katalog, behandling og lagring av informasjon

Klassifiseringen av data har betydning for hvor og hvordan data skal behandles og lagres. Data kan bare lagres og behandles i IT-tjenester som er godkjent for den aktuelle klassen. IT-katalogen har oversikt over hvilke IT-tjenestene og klassene de er godkjent for.

Bestemme data og informasjonsklasse

Data skal alltid plasseres i en tilstrekkelig sikker dataklasse. Dersom du er i tvil om du skal velge f.eks. rød eller gul, skal du velge rød. Klassene er beskrevet i dataklassetabellen under.

Data og informasjonsansvarlig

Alle data og all informasjon skal ha en informasjonsansvarlig som er entydig og identifiserbar.

Informasjonsansvarlig skal:

- sikre at data er plassert i riktig dataklasse ut ifra disse reglene
- sørge for at alle som skal behandle data er informert om hvilken dataklasse som skal brukes
- vurdere når data og informasjon bytter dataklasse
- påse at all lagring, behandling og bearbeiding av data foregår på tekniske løsninger som er godkjent for dette – se IT-katalog
- regelmessig sjekke at man oppfyller eventuelle endringer i kravene

Dataklasser

Dataklasser	Beskrivelse	Tilgjengelighet
	**Grønn** Grønn er åpen informasjon er dokumenter og data eller opplysninger som kan være tilgjengelige for alle uten noen tilgangsbegrensninger og som ikke krever spesielle sikkerhetstiltak. **Potensiell skade (MAPS, 2025)** • Lav Data kan være lisensiert med begrensninger for bruk.	Kan eller skal være tilgjengelig for alle. Integritet skal sikres.
	**Gul** Gul informasjon er dokumenter og data som er kontrollert og ikke åpen for alle, men som ikke er like sensitiv som rød informasjon og derfor krever mindre strenge sikkerhetstiltak. **Potensiell skade (MAPS, 2025)** • Mindre alvorlig	Begrenset. Kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter.
	**Rød** Rød er dokumenter og data vi er pålagt å begrense tilgang til gjennom lover, regler, avtaler og beskyttelse av kommersielle interesser. **Potensiell skade(MAPS, 2025)** Alvorlig til kritisk	Begrenset
	**Blå** Spesialklasse for M365. Basert på rød klasse, men som også sperrer for Copilot sin tilgang til dokumentet. Blå er dokumenter og data vi er pålagt å begrense tilgang til gjennom lover, regler, avtaler og beskyttelse av kommersielle interesser. **Potensiell skade (MAPS, 2025)** Alvorlig til kritisk	
	**Svart-P** Svarte-P er samme type dokumenter og data som rød. Altså data vi er pålagt å begrense tilgang til gjennom lover, regler, avtaler og beskyttelse av kommersielle interesser. Det spesielle er at en ønsker å beskytte dataene ytterligere, og ofte fordi omfanget (data mengden) er betydelig større. P-data er data som inneholder personopplysninger. **Potensiell skade (MAPS, 2025)** • Kritisk til meget kritisk Pålegg om beskyttelse og sikring utover de lovbestemte skal være nedfelt i avtaler eller skriftlig dokumentert på annen måte. Personvernforordning (GDPR) Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.	Strengt begrenset
	**Svart-S** Omfatter samme type data som rød, men der spesielle hensyn gjør at man ønsker å beskytte dataene ytterligere. Altså data vi er pålagt å begrense tilgang til gjennom lover, regler, avtaler og beskyttelse av kommersielle interesser. Det spesielle er at en ønsker å beskytte dataene ytterligere, og ofte fordi omfanget (data mengden) er betydelig større. **Potensiell skade (MAPS, 2025)** • Kritisk til meget kritisk Pålegg om beskyttelse og sikring utover de lovbestemte skal være nedfelt i avtaler eller skriftlig dokumentert på annen måte. Data som er omfattet av eksportkontroll lov og forskrift.	Strengt begrenset
	**Grå** Data som er sikkerhetsgradert. Denne data klassen kan ikke lagres i NORCE sin IT-plattform.	Data må oppbevares og behandles i kunde eller oppdragsgiver sine systemer.

Guidelines for classification and storage of data and information

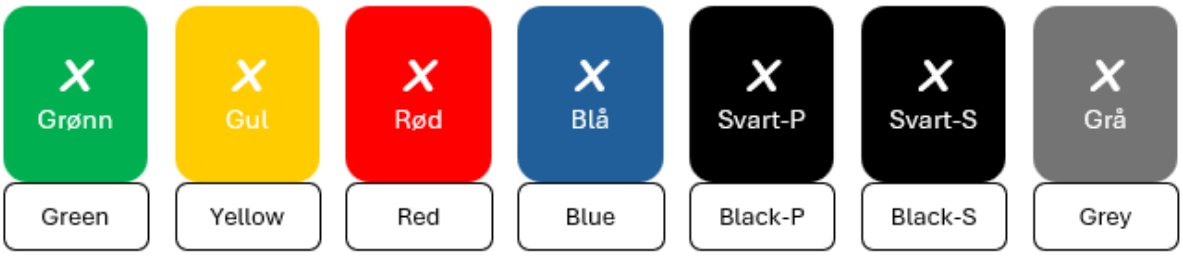
Purpose and scope

Data classification is necessary to ensure the confidentiality, integrity and availability of data and information. The guidelines apply to all data and information that NORCE processes and stores.

Processing and storage of data and information means all data, files, information and documents that are created, processed and stored by NORCE, and which we must therefore ensure responsible processing and storage of. Examples are all administrative data and project data such as Word and Excel documents, e-mail and all research data.

The guidelines are based on a common standard in the university and college sector.

Our data classes:



IT services: IT catalog, processing and storage of information

The classification of data has an impact on where and how data is processed and stored. Data can only be stored and processed in IT services that are approved for the relevant class. The IT catalogue provides an overview of which IT services and classes they are approved for.

Decide data and information class

Data must always be placed in a sufficiently secure data class. If you are in doubt about whether to choose e.g., red, or yellow, select red. The classes are described in the data class table below.

Data and information controller

All data and information must have a clear and identifiable information controller.

The information controller:

- ensure that data is placed in the correct data class based on these rules
- ensure that everyone who processes data is informed about which data class shall be used
- assess when data and information change data class
- ensure that all storage, processing and processing of data takes place on technical solutions that are approved for this – see IT catalogue
- regularly check that any changes in the requirements are met

Data classes

Data classes	Description	Availability
	**Green - Open** Open information is documents and data or information that can be accessed by anyone without any access restrictions and that does not require special security measures. **Potential damage (MAPS, 2025)** • Low The data may be licensed with restrictions on use.	Can or should be available to everyone. Integrity must be ensured.
	**Yellow** Restricted information is documents and data that are controlled and not open to everyone but are not as sensitive as confidential information and therefore require less stringent security measures. **Potential damage (MAPS, 2025)** • Less serious	Restricted It can be available to both external and internal users, with controlled access rights.
	**Red** Red are documents and data to which we are required to restrict access through laws, regulations, agreements and the protection of commercial interests. **Potential damage (MAPS, 2025)** Severe to critical	Limited
	**Blue** Based on red class, but also block for Copilot Blue are documents and data to which we are required to restrict access through laws, regulations, agreements and the protection of commercial interests. **Potential damage (MAPS, 2025)** Severe to critical	
	**Black-P** Black-P is the same type of data as red. That is, data that we are required to restrict access to through laws, regulations, agreements and protection of commercial interests. The special thing is that one wants to protect the data further, and often because the scope (data volume) is significantly larger. P-data is data that contains personal data. **The protection instruction** (Lovdata.no, 1972) • Strictly in confidence **Potential damage (MAPS, 2025)** Critical to very critical Orders for protection and security beyond those required by law must be laid down in agreements or otherwise documented in writing. General Data Protection Regulation (GDPR) Norm for information security and privacy in the health and care sector.	Strictly limited.
	**Black-S** Black is the same type of data as red. That is, data that we are required to restrict access to through laws, regulations, agreements and protection of commercial interests. The special thing is that one wants to protect the data further, and often because the scope (data volume) is significantly larger. **Potential damage (MAPS, 2025)** Critical to very critical Orders for protection and security beyond those prescribed by law shall be set out in agreements or otherwise documented in writing. Data covered by export control laws and regulations.	Strictly limited.
	**Gray - Security graded** Data in this category cannot be stored in the NORCE IT platform. Typical security graded information.	Data must be stored and processed in the customer's or client's systems.

Referanser / References

Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen), (1972). https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352

Lov om nasjonal sikkerhet (Sikkerhetsloven), (2018). https://lovdata.no/dokument/NL/lov/2018-06-01-24

MAPS. (2025). *L2. NORCE risikokriterier og mulighetsrangering*. https://norce.sharepoint.com/sites/MAPS/docs/l2-risiko/norce-risikokriterier-mulighetsrangeringer.xlsx