

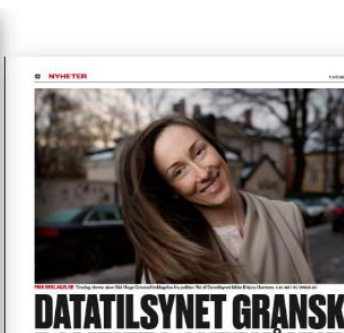


Personvernombud – Data protection officer

Rolf Jegervatn

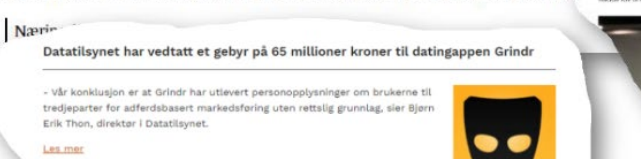
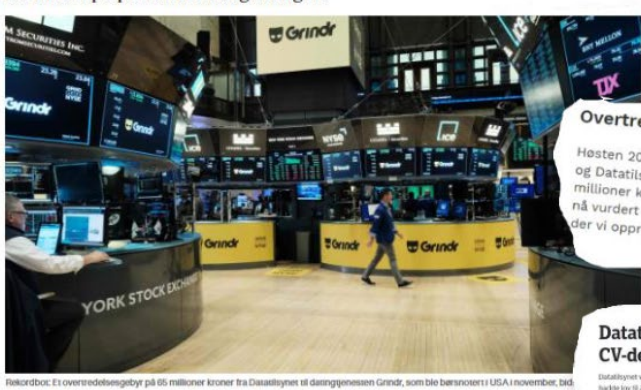


Privacy and GDPR have public interest



Datatilsynet håvet inn på personvernbrudd i fjor

I år er det fem år siden personvernforordningen (GDPR) fortsatt synder både offentlige og private virksomheter. I i fjor ut samlede overtredelsesgebyrer på nærmere 100 millioner kroner for brudd på personvernlovgivningen.



Gebyr til Trumf

Datatilsynet har fattet vedtak om overtredelsesgebyr på fem millioner kroner til Trumf. Bakgrunnen for gebyret er at Trumf-medlemmer kunne registrere andres kontonummer på medlemsprofilen og dermed skaffe seg tilgang til andres handlehistorikk.

Overtredelsesgebyr til Stortinget

Høsten 2020 ble Stortinget utsatt for datainnbrudd og Datatilsynet varslet i januar et gebyr på to millioner kroner for manglende sikkerhetsnivå. Vi har nå vurdert Stortingets merknader og sendt vedtak der vi opprettholder det varslede gebyret.



What does GDPR protect

Increased control for the individual:













How are our personal data used?

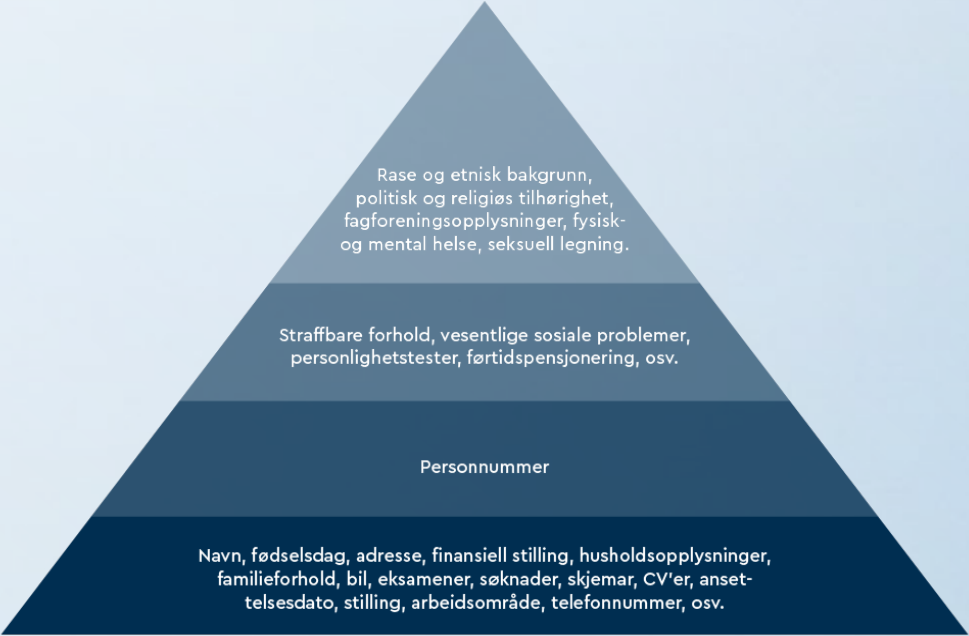
How are they shared?

How are they stored?

Article 4 of the Personal Data Act deals with ordinary personal data.

Articles 9 and 10 deal with special categories of personal data.

GDPR: Types of Data under Protection	
Personal Data	Sensitive Personal Data
 Names	 Health Data
 Location Data	 General Data
 Identification Numbers	 Biometric Data
 IP Addresses	 Racial or Ethnic Data
 Cookie Data	 Political Opinions
 RFID Tags	 Sexual Orientation



7 Principles of data protection law

Protecting personal data:

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

The requirements in the GDPR framework are based on the 7 principles – the core of GDPR.

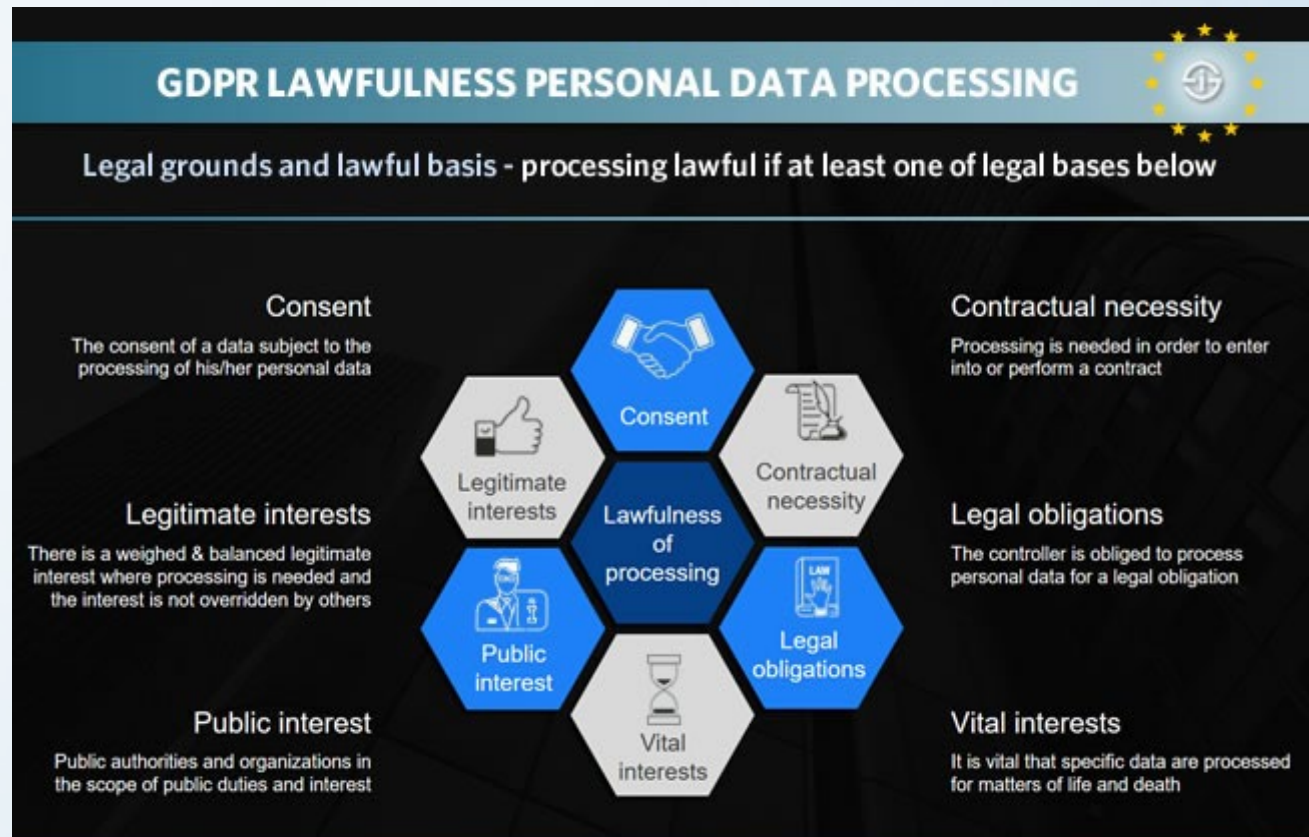
- The key principles related to the processing of personal data are further described in GDPR Art. 5



Legal basis for processing personal data

Article 6 - GDPR defines the six lawful bases that data controllers can leverage for the processing of personal data.

- Legal basis 1: Informed consent (Art. 6(1)(a) – often used in research
- Legal basis 2: Contractual Necessity
- Legal basis 3: Legal Obligation
- Legal basis 4: Protection of Vital Interests
- Legal basis 5: Task Carried Out in the Public Interest or in the Exercise of Official Authority- (Art. 6(1)(e))
- Legal basis 6: Legitimate Interests:

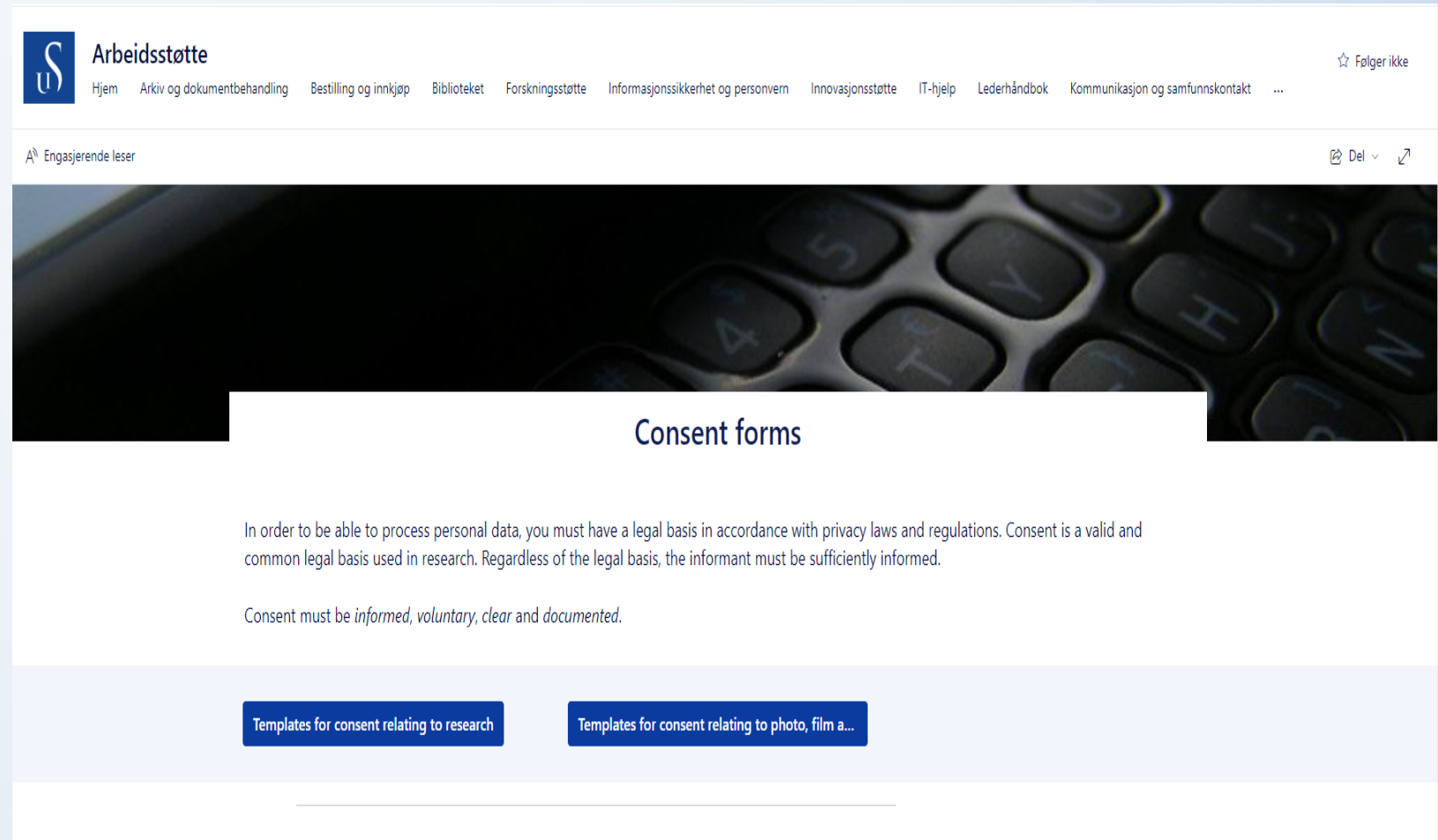


Legal basis for processing personal data in research

- Legal basis 1: Informed consent (Art. 6(1)(a))
- Legal basis 5: Task Carried Out in the Public Interest or in the Exercise of Official Authority- (Art. 6(1)(e))

In addition:

- Article 9(2)(j) and Article 89(1)
- <https://liveuis.sharepoint.com/sites/Arbeidsstoette/SitePages/Consent-forms-and.aspx>
- [Personverntjenester for forskning \(sikt.no\)](https://sikt.no)



Arbeidsstøtte

Hjem Arkiv og dokumentbehandling Bestilling og innkjøp Biblioteket Forskningsstøtte Informasjonssikkerhet og personvern Innovasjonsstøtte IT-hjelp Lederhåndbok Kommunikasjon og samfunnskontakt ...

Engasjerende leser

Consent forms

In order to be able to process personal data, you must have a legal basis in accordance with privacy laws and regulations. Consent is a valid and common legal basis used in research. Regardless of the legal basis, the informant must be sufficiently informed.

Consent must be *informed, voluntary, clear and documented*.

Templates for consent relating to research

Templates for consent relating to photo, film a...

What is a breach in the processing of personal data

GDPR defines it as: unintentional or unlawful destruction, loss, alteration, illegal disclosure, or access to personal data that has been transmitted, stored, or otherwise processed.

A personal data breach consists of three elements:

1. Security breach
2. Leading to unintentional or unlawful destruction, loss, alteration, illegal disclosure, or access (causality)
3. The breach involves personal data

Categories of personal data breaches:

1. Breach of **confidentiality**, meaning there has been unintentional or unlawful disclosure or access to personal data.
2. Breach of **integrity**, meaning there has been unintentional or unlawful alteration of personal data.
3. Breach of **availability**, meaning there has been unintentional or unlawful loss of access to or deletion of personal data.

A breach can encompass one or a combination of these three categories."



Recommendations from DPO

- Define the purpose of collecting and using personal data and know what the legal basis for processing is.
- Process personal data only with a legal basis
- Be transparent about how you process your data
- Act in line with the rights of data subjects – Respondents, rights?
- Classification of what you are processing, and knowledge of storage tools, is important before collecting data.
- Good planning and familiarity with guides/intranet resources facilitate secure data management.
- Ensure protection of your data, wherever stored, minimise where you can and share under the right conditions
- Nettskjema is the primary data collection tool for surveys and audio recordings, up to sensitive data (red category).
- Remember to delete personal data after the intended purpose is fulfilled.
- Report deviations!
- Thank you for your attention!



Useful Sources

- [UiS intranet](#)
- [Datatilsynet](#)
- [SIKT](#)