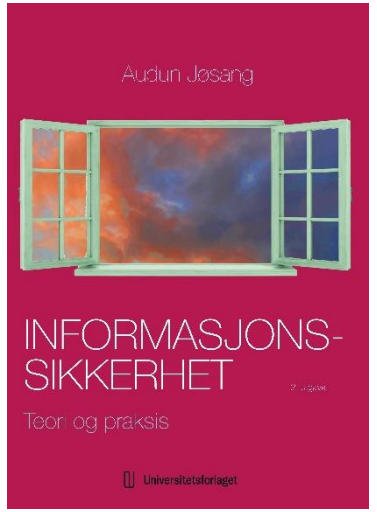
Kapittel 10: Personopplysningsvern og GDPR

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Personvern og personopplysningsvern

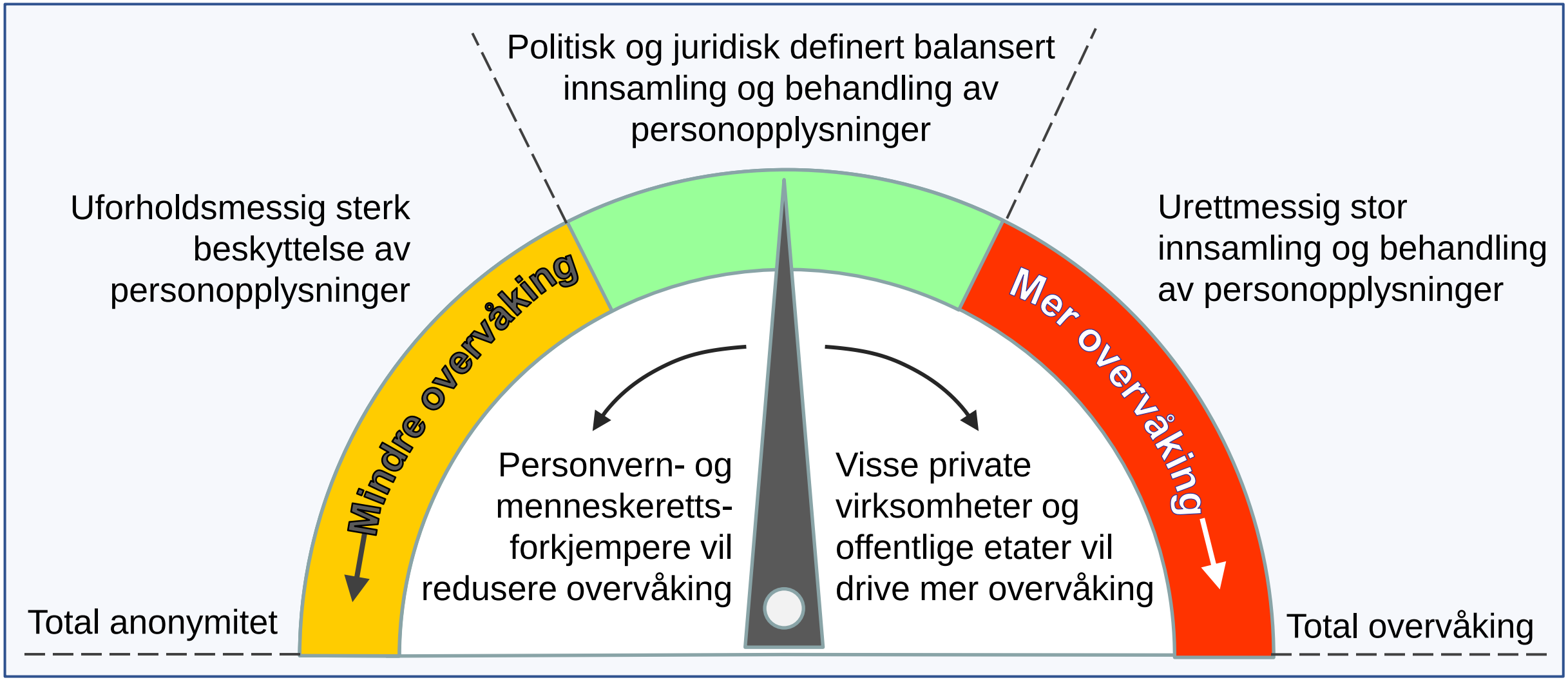
Grunnloven § 102: Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

Personvern

Personopplysningsvern

- Personvern (eng. Privacy) er et generelt begrep som er uttrykt i den europeiske menneskerettskonvensjon, FNs menneskerettserklæring og grunnloven § 102
- Personopplysningsvern (eng. Data Protection) iht. GDPR er en underkategori av personvern rettet mot beskyttelse av personopplysninger (eng. personal data).
- På norsk kaller vi «personopplysningsvern» for «personvern» fordi det er kortere.

Overvåkingsbarometer

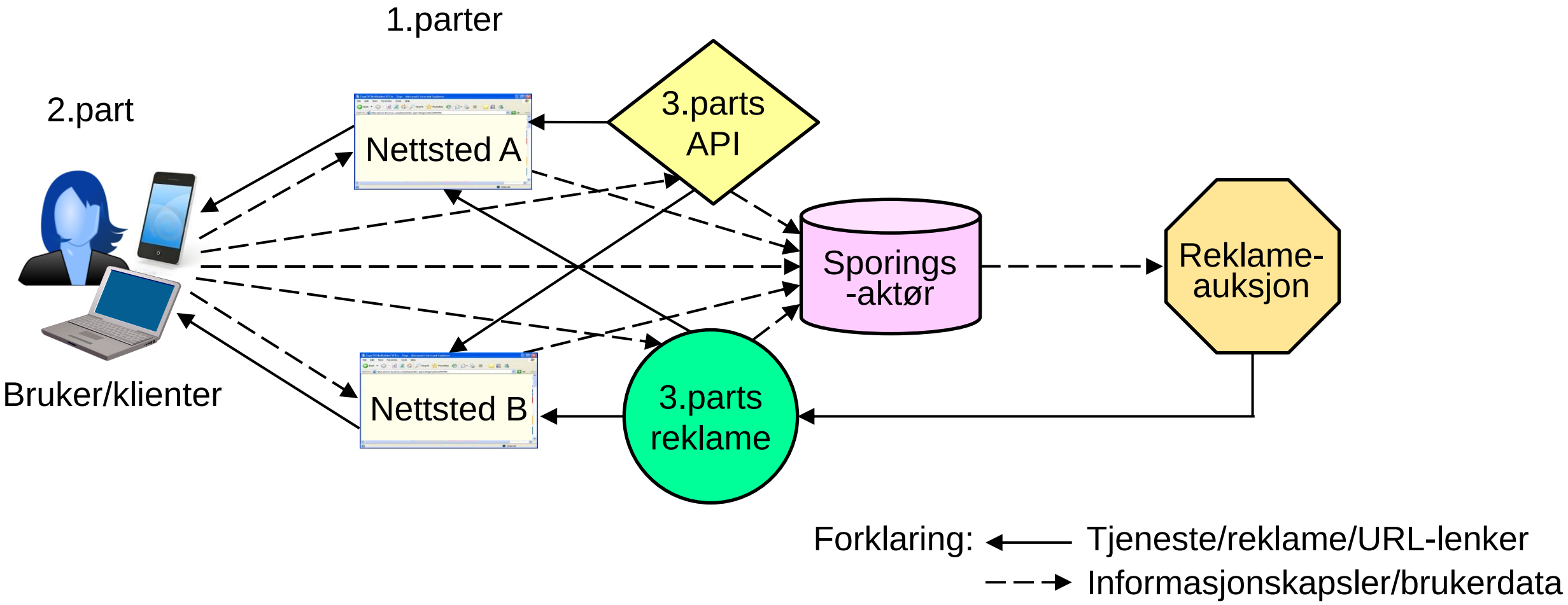


Behov for balanse mellom personvern og overvåking

- La oss først betrakte en tilstand med massiv innsamling av personopplysninger
  + Det kan støtte nye forretningsprosesser, effektivisere forvaltningen og gjøre våre liv enklere
  + Gir politimyndigheter enorme muligheter for å etterforske kriminalitet og håndheve lov og orden.
  – Vil krenke vår integritet, skape uønsket oppmerksomhet, gjøre at vårt privatliv blir utlevert
  – Kan føre til diskriminering, maktmisbruk og undertrykking som kan true vårt demokrati.
- La oss så betrakte en tilstand med minimal innsamling av personopplysninger
  + Vi kan være i fred for uønsket oppmerksomhet fra kommersielle selskaper
  + Vi får mindre grunn til å frykte maktmisbruk og undertrykking fra myndighetene.
  – Det vil hemme utvikling av smarte forretningsprosesser, gjøre forvaltning ineffektiv
  – Det vil forhindre effektiv etterforskning av kriminalitet. Å gi uforholdsmessig sterkt personvern til kriminelle og terrorister lammer håndheving av lov og orden, som igjen kan true vårt demokrati..

– Konklusjon: Vi trenger en god balanse mellom personvern og overvåking

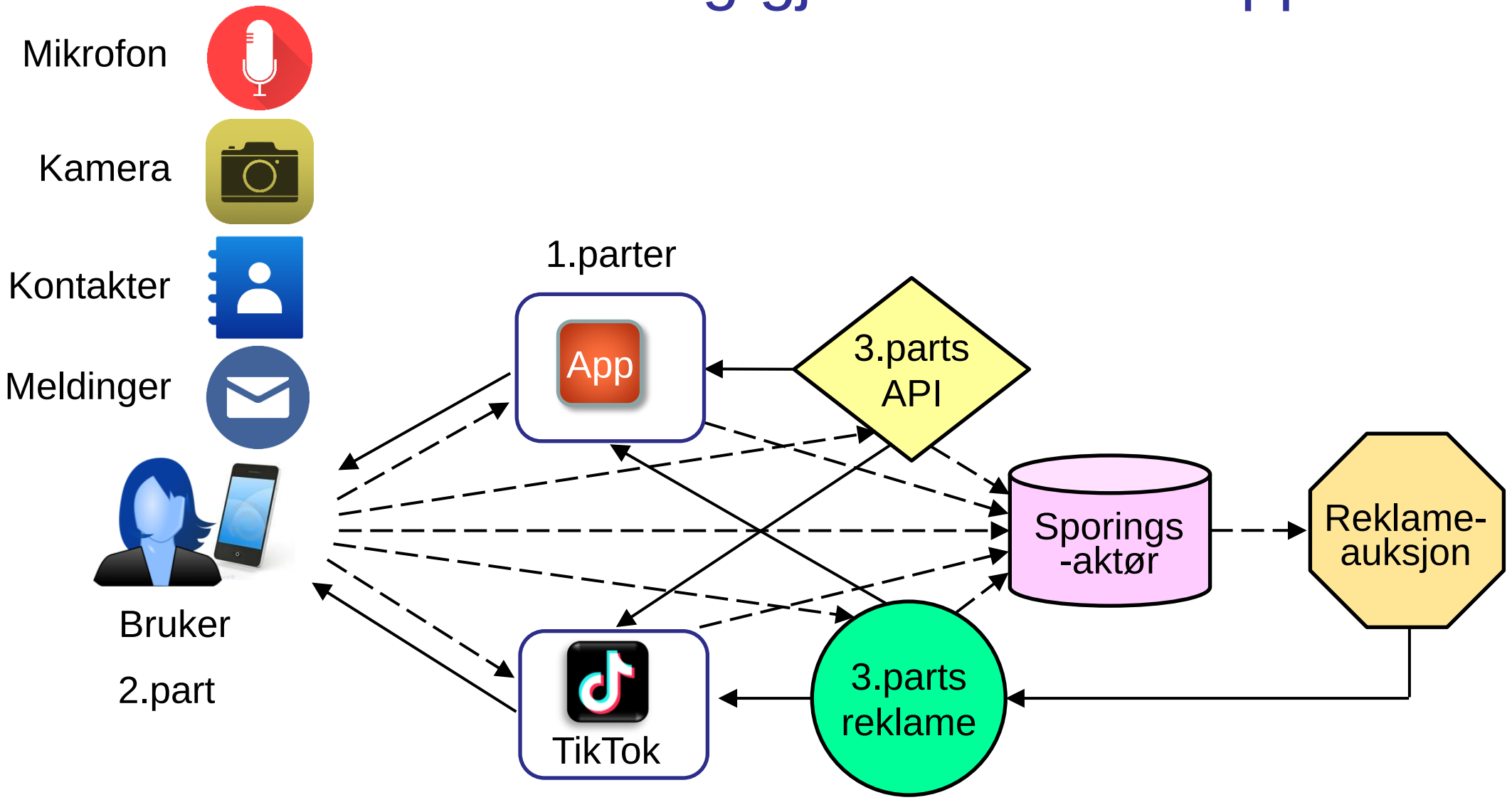
Overvåking på nett



Reklameauksjoner på web

- Nettsteder samler inn informasjon om brukere over tid, bl.a. med infokapsler
- Tilleggsfunksjoner gjennom tredjeparts-API-er samler også info in brukere.
- Sporingsaktører lager profiler om brukere gjennom aggregering av info
- Nettsteder som sender en webside til nettleseren, legger inn URL-lenker til reklame og andre ting som nettleseren selv laster inn fra tredjeparter.
- Reklamen bestemmes gjennom auksjoner som foregår mens nettsiden laster
  1. Auksjonen åpnes ved at annonsører mottar en budutlysning om en nettside som en bruker har klikket på. Annonsører mottar brukerprofilen, slik at de kan vurdere relevans.
  2. Annonsører definerer hver sin budstrategi ut ifra hvor relevant brukeren er for dem.
  3. Til slutt vinner den høystbydende annonsør auksjonen, og formidler automatisk reklamen som integreres i nettsiden som presenteres til brukeren, i håp om at brukeren ser og kanskje klikker på reklamen.

Overvåking gjennom mobilapper



Apper som invaderer personvern og overvåker

- Mobilapper krever som regel tilgang til forskjellige ressurser på mobilenheten, som kontakter, bilder, mikrofon, kamera, og lokasjon.
- Vi samtykker ofte til alt en mobilapp ber om uten å tenke så mye over det, fordi vi ønsker å ta appen i bruk så fort som mulig, og tenker at ressursene trengs.
- Teknisk sett kan apper …
  - aktivere kamera og mikrofon når som helst,
  - sende lyd, bilde, meldinger, adresser, bilder og filer til app-eieren, f.eks. for å spionere
- I mars 2023 kom anbefaling fra Justis- og beredskapsdepartementet og NSM om at statlig ansatte ikke får installere appene TikTok og Telegram på sine mobiltelefoner og andre digitale enheter eid av arbeidsgiveren.
- TikTok og Telegram som alle andre apper bortsett fra at TikTok er kinesisk-eid og Telegram er russisk-eid, og at Kina og Russland regnes som trusselaktører.
- Kinesiske virksomheter er forpliktet til å utlevere info som myndighetene ber om.

LOVDATA

Søk etter lover, forskrifter, dommer og stortingsvedtak

Rettskilder

- Lover
- Stortingsvedtak
- Sentrale forskrifter
- Lokale forskrifter
- Norsk Lovtidend
- Norges traktater
- Dommer
- Statens personalhåndbok
- Oversatte lover /

Lov om behandling av personopplysninger (personopplysningsloven)

➡ Gå til opprinnelig kunngjort versjon

Lov om behandling av personopplysninger (personopplysningsloven)

Dato	LOV-2018-06-15-38
Departement	Justis- og beredskapsdepartementet
Sist endret	LOV-2018-12-20-116
Ikrafttredelse	20.07.2018
Endrer	LOV-2000-04-14-31
Kunngjort	15.06.2018
Rettet	11.02.2019 (GDPR art 40)
Korttittel	Personopplysningsloven

Person(opplysnings)vern

Personopplysninger (eng. Personal Data, eller PII: Personally Identifiable Information) er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.

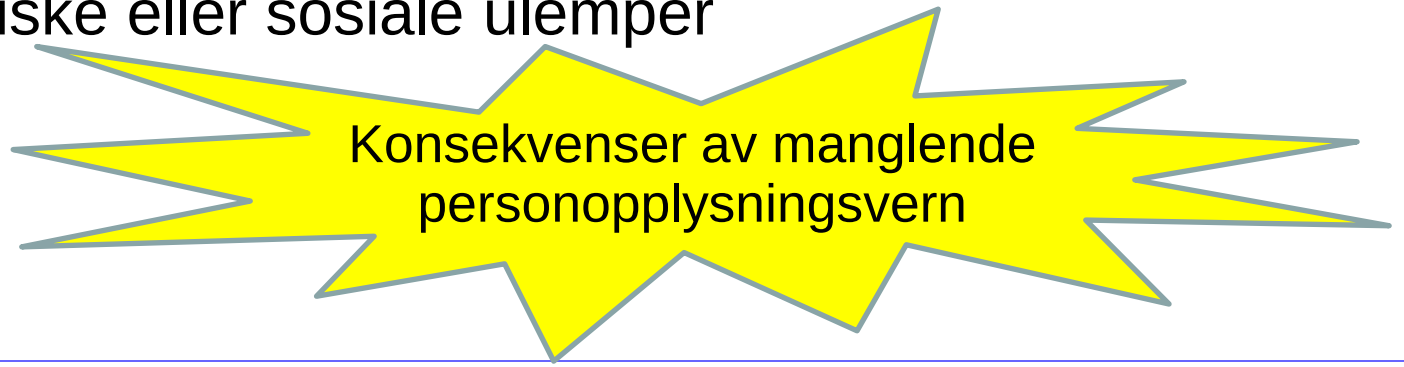
Begrepet «personopplysning» er ekvivalent med persondata eller personinformasjon.

Person(opplysnings)vern er å beskytte spesifikke aspekter ved personopplysninger:

- Forhindre urettmessig innsamling og oppbevaring av personinformasjon
- Forhindre urettmessig bruk av innsamlet personinformasjon
- Sørge for at personinformasjon er korrekt
- Sørge for åpenhet og innsyn
- Sørge for adekvat informasjonssikkerhet (KIT) rundt personinformasjon
- Definere klar ansvarsfordeling

Mulige konsekvenser av mangelfullt personvern

- Personlig belastning
- Uønsket oppmerksomhet
- Forskjellsbehandling
- Identitetstyveri eller –bedrageri
- Økonomisk tap
- Skade på omdømme
- Tap av fortrolighet for taushetsbelagte personopplysninger
- Uautorisert oppheving av pseudonymisering
- Andre økonomiske eller sosiale ulemper

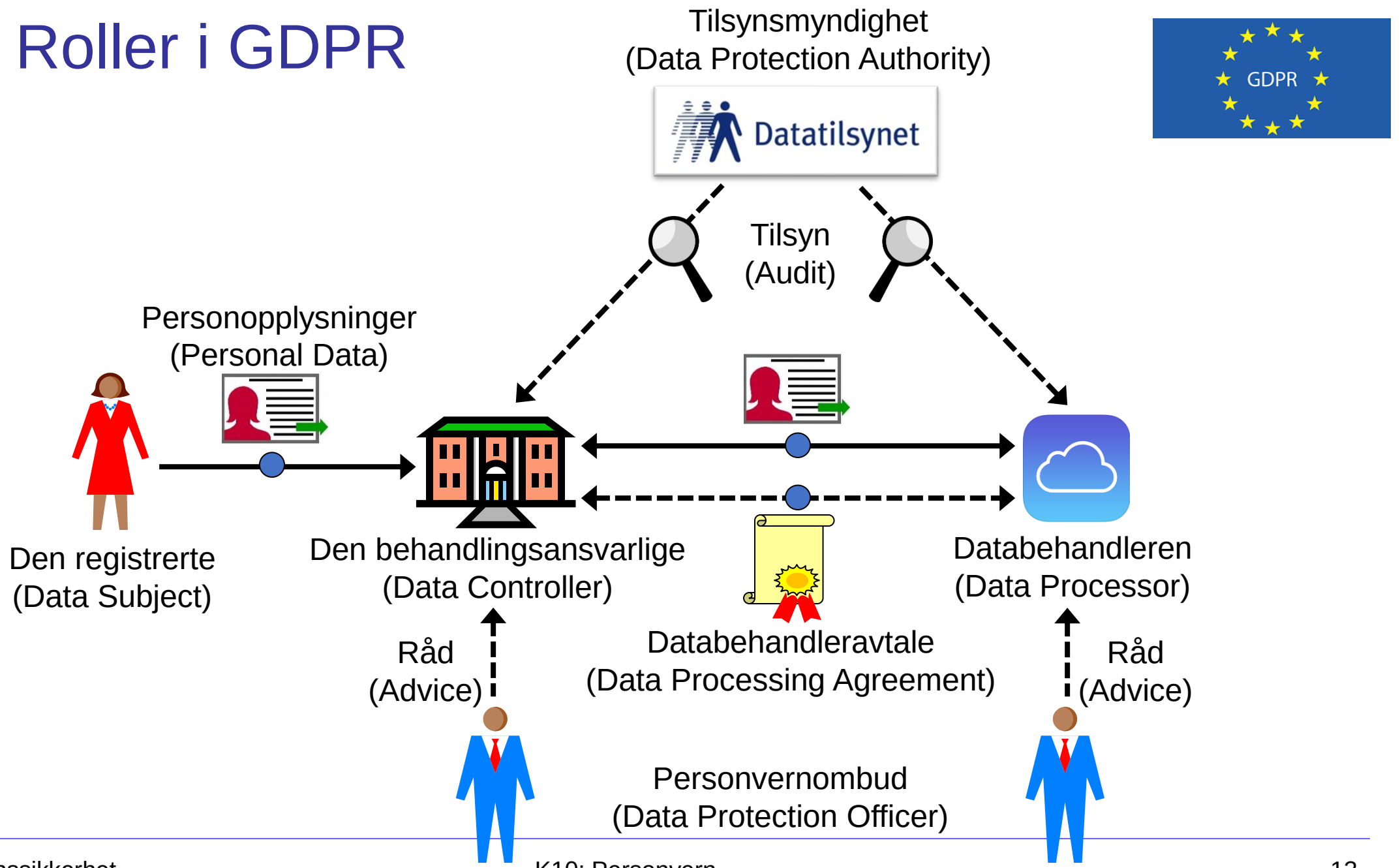


General Data Protection Regulation (GDPR)

på norsk: Personvernforordningen (PVF)

- Trådte i kraft som lov i EU 25.05.2018, i Norge 20.07.2018, kalles som regel GDPR.
- Håndheves av hvert lands tilsynsmyndighet, som er Datatilsynet i Norge.
- EUs lovtekst (GDPR) oversatt til norsk uten endring, 99 artikler .
- Følgende artikler presenteres her:
  - Art. 5: Prinsipper for behandling av personopplysninger
  - Art. 6: Behandlingens lovlighet (behandlingsgrunnlag)
  - Art. 25: Innebygd personvern
  - Art. 32: Sikkerhet ved behandlingen (innebygd informasjonssikkerhet)
  - Art. 35: Vurdering av personvernkonsekvens (DPIA)
  - Art. 45: Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå
  - Art. 46: Overføringer som omfattes av nødvendige garantier
  - Art. 83: Generelle vilkår for ilegging av overtredelsesgebyr

Roller i GDPR



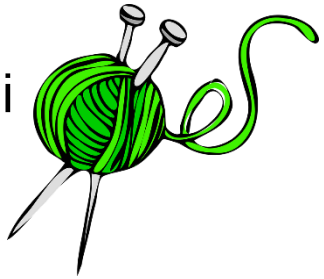
Eksempler på personopplysninger

Identitet: Navn, fødselsnummer, sivilstatus, høyde, vekt, passfoto, fingeravtrykk

Finans: Inntekt, skatt, gjeld, bankkonto, kontoutskrift, utgifter, kredittvurdering etc.

Kontaktinfo: Hjemmeadresse, jobbadresse, mobilnummer, epostadresse, brukernavn, etc.

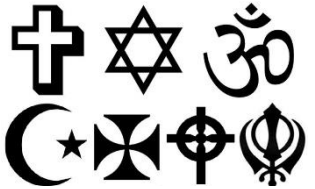
Pseudonymiserte opplysninger:
Kvinne, 43 år, Oslo, liker å strikke, har sibirkatt, jobber i offentlig etat, to barn.



Aktivitet: Adferdsmønstre, interesser hobbyer, studier, yrkesliv, lokasjon posisjon, kjøpemønster, søkehistorikk, etc

Kommunikasjon: MAC- og IP-adresse, SMS, MMS, fotografier, videoer, sosialt nettverk, kontakter, cookies etc.

Særlige kategorier: Helseopplysninger, fagforeningsmedlemskap, politisk oppfatning, religion, seksuelle forhold/orientering, etnisitet/rase



Art. 5: Prinsipper for behandling av personopplysninger

1. *Personopplysninger skal behandles med:*
   a) *Lovlighet, rettferdighet og åpenhet*
   b) *Formålsbegrensning*
   c) *Dataminimering*
   d) *Riktighet*
   e) *Lagringsbegrensning*
   f) *Integritet og konfidensialitet*

2. *Den behandlingsansvarlige har ansvar for pkt. 1 ovenfor.*

Art. 6: Behandlingens lovlighet (behandlingsgrunnlag)

1. *Behandlingen er bare lovlig når minst ett av følgende vilkår er oppfylt:*
   - *a) den registrerte har samtykket til behandling for ett eller flere spesifikke formål,*
   - *b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,*
   - *c) behandlingen er nødvendig for å oppfylle behandlingsansvarliges rettslig forpliktelser,*
   - *d) behandlingen er nødvendig for å verne den registrertes eller andre personers vitale interesser,*
   - *e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,*
   - *f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*

     Punkt f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver (fordi dette tilfellet dekkes av punkt e)).

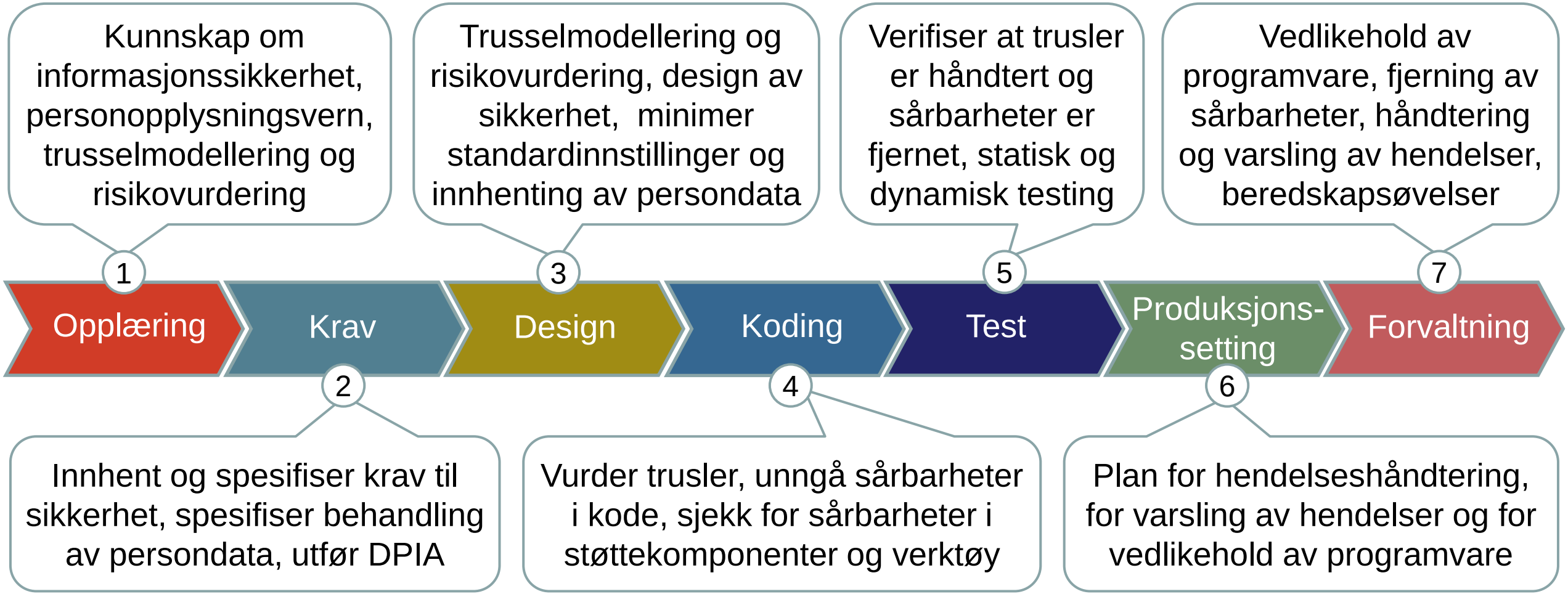
Art. 6.1.f: Behandlingsansvarliges berettigede interesser

- GDPR Art. 6.1.f kan virke som en «blankofullmakt» for behandling av personopplysninger, men det er det ikke.
- For å kunne anvende Art. 6.1.f som behandlingsgrunnlag må behandlingsansvarlig kjøre en test med 3 punkter, der det må svares Ja på alle 3:
  1. **Formålstest:** Ligger det en berettiget interesse bak behandlingen?
  2. **Nødvendighetstest:** Er behandlingen nødvendig for det formålet?
  3. **Balansetest:** Bør den registrertes interesser eller grunnleggende rettigheter og friheter vike for den behandlingsansvarliges berettige interesser?
- Eksempel på anvendelse av Art. 6.1.f: *Avdekke forsikringssvindel,* med test:
  1. Forsikringsselskaper har faktisk en berettiget interesse av å forhindre svindel.
  2. Behandling av spesifikke personopplysninger relatert til kunder er faktisk nødvendig for dette.
  3. Den registrertes interesser for å ikke ha personopplysninger behandlet av forsikringsselskaper synes ikke å veie tyngre enn forsikringsselskapenes berettige interesse av å forhindre svindel.

Art. 25: Innebygd personvern og personvern som standardinnsstilling

1. *Det skal gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering.*
2. *Det skal gjennomføres egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare behandles personopplysninger som er nødvendige for spesifikke formål. Dette gjelder mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet.*

Innebygd personvern og informasjonssikkerhet

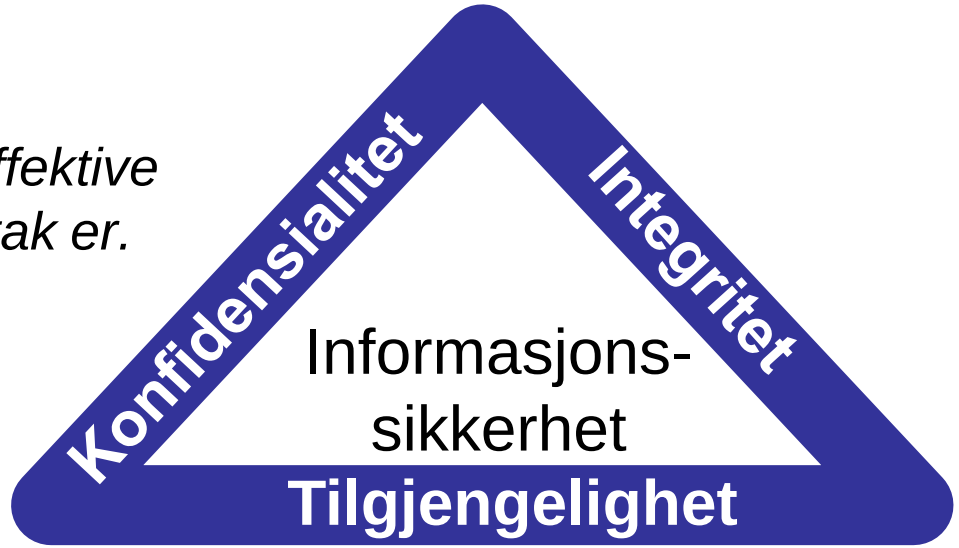


Veileder fra Datatilsynet

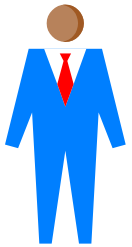
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Art. 32: Sikkerhet ved behandlingen

1. *Det skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen, herunder blant annet:*
   a) *pseudonymisering og kryptering av personopplysninger*
   b) *evne til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,*
   c) *evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid ved tekniske hendelser,*
   d) *regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.*



Personvernombud



Personvernombudet gir råd til behandlingsansvarlige eller databehandleren om forpliktelser som virksomheten har etter personvernloven. Alle virksomheter kan ha personvernombud.

Personvernombud må oppnevnes når:

- Behandlingen utføres av en offentlig myndighet.
- Databehandlingen har en art, omfang og/eller formål som krever regelmessig og systematisk monitorering i stor skala.
- Behandlingsansvarliges eller databehandlerens hovedvirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 (sensitive personopplysninger) eller personopplysninger knyttet til straffedommer og straffbare forhold som er nevnt i artikkel 10.

Art. 45: Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå

1. *Personopplysninger kan overføres til en tredjestat eller en internasjonal organisasjon når Kommisjonen har fastslått at tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat eller den aktuelle internasjonale organisasjonen sikrer et tilstrekkelig beskyttelsesnivå. En slik overføring skal ikke kreve en særlig godkjenning.*
2. *Ved vurderingen av om beskyttelsesnivå er tilstrekkelig skal Kommisjonen særlig ta hensyn til det følgende:*
   a) *prinsippet om rettsstaten*
   b) *om det finnes en eller flere velfungerende, uavhengige tilsynsmyndigheter i tredjestaten*
   c) *de internasjonale forpliktelsene som den berørte tredjestaten har påtatt seg*
3. *Etter å ha vurdert om beskyttelsesnivået er tilstrekkelig, kan Kommisjonen beslutte at en tredjestat sikrer et tilstrekkelig beskyttelsesnivå i henhold til nr. 2 i denne artikkel (adekvansbeslutning).*

Land som omfattes av adekvansbeslutning

- Adekvansbeslutning for en stat eller område betyr at overføringen vil være sammenlignbar med overføringer mellom land innenfor EØS.
  - gjør overflødig å definere annet overføringsgrunnlag eller godkjenning fra Datatilsynet.
- Per 2023 gjelder adekvansbeslutning for følgende land:

Andorra	Argentina	Guernsey	Isle of Man
Israel	Jersey	New Zealand	Sveits
Storbritannia	Uruguay		

- Under gitte betingelser gjelder adekvansbeslutning også for følgende land:

Canada	Færøerne	Japan	Sør-Korea
USA			

- Se info fra Datatilsynet:
  - https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/

Schrems-II dommen

- Max Schrems anklaget EU fordi han mente at adekvansbeslutning for USA basert på *Privacy Shield-avtalen* var brudd på GDPR, pga. følgende lover:
  - FISA Section 702 (Foreign Intelligence Surveillance Act) åpner for å innhente etterretning om ikke-amerikanske personer som ikke befinner seg i USA.
  - Executive Order 12333 regulerer all amerikansk utenlandsk etterretningsvirksomhet, inkludert aktiviteter som faller utenfor FISA, f.eks. utført utenlands mot ikke-amerikanske personer. Etterretningsvirksomheten kan foregå hemmelig.
  - Presidential Policy Directive 28 åpner for masseinnhenting av (person)data for overvåking uten at berørte personer er spesifikt mistenkt eller utpekt som interessante. Dog kan innhentede data kun benyttes for nasjonal sikkerhet, og ikke f.eks. til industrispionasje.
- 16. juli 2020 vant Max Schrems rettsaken, og *Privacy Shield* ble opphevet.
- Etter dommen måtte overføring til USA være basert på GDPR Art.46 og Art.47.
- 10. juli 2023 ble det etablert en ny avtale kalt *EU – US Data Privacy Framework*
  - Igjen er det gjort en adekvansbeslutning for overføring til USA for amerikanske virksomheter som er sertifisert under denne avtalen. Max Schrems har varslet anklage mot den nye avtalen.
-

Art. 46: Overføringer som omfattes av nødvendige garantier

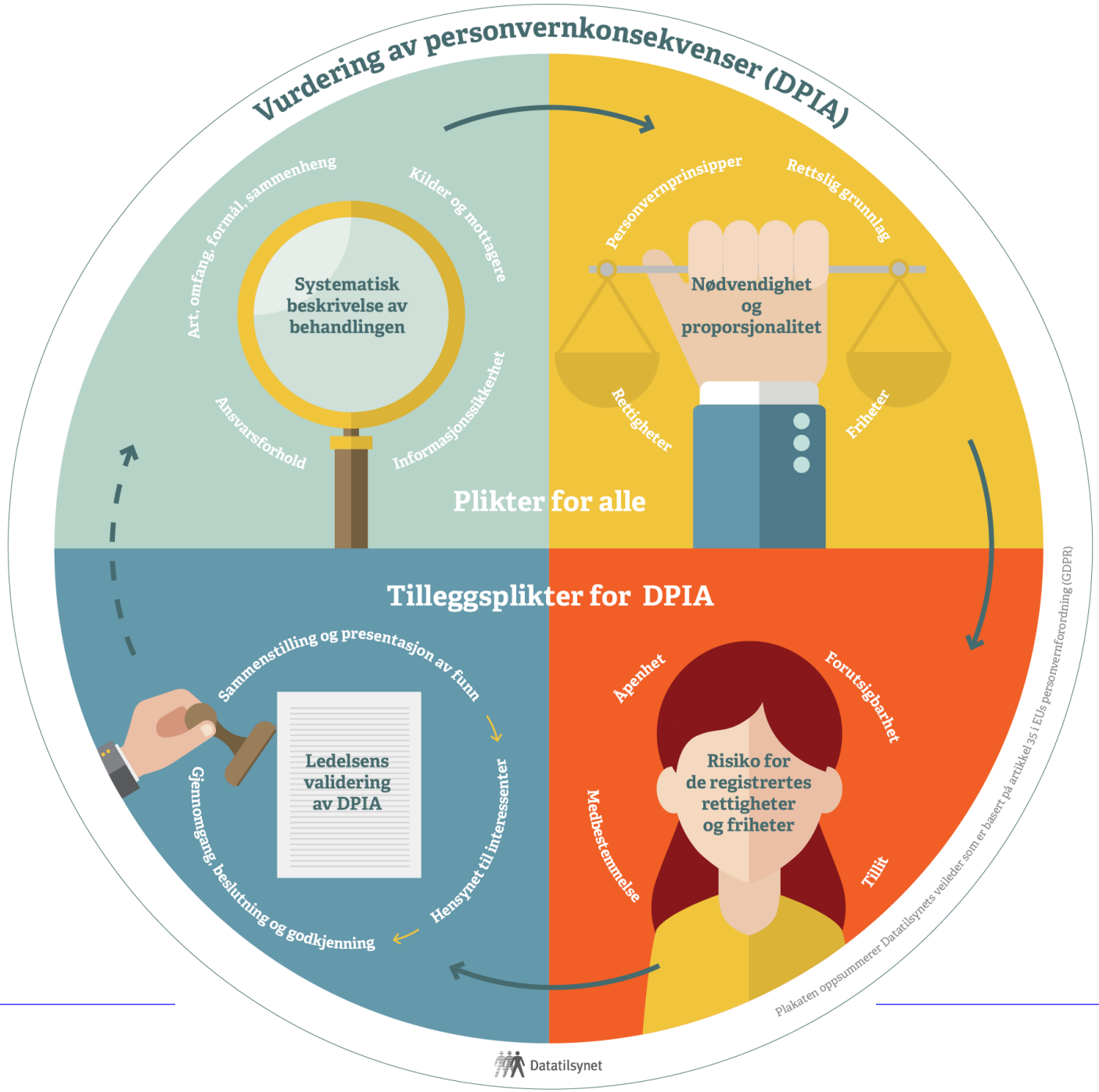
1. *Dersom det ikke foreligger en beslutning i henhold til Art. 45 nr. 3, kan en behandlingsansvarlig eller databehandler overføre personopplysninger til en tredjestat eller en internasjonal organisasjon bare dersom behandlingsansvarlig eller databehandleren har gitt nødvendige garantier, og under forutsetning av at de registrerte har håndhevbare rettigheter og effektive rettsmidler.*

- Bruk av amerikanske skytjenester, som f.eks. Office 365, må vurderes utifra GDPR Art. 46. Elementer som må vurderes er f.eks.:
  - Sensitivitet av personopplysningene.
  - I hvilken grad innhenting og behandling av personopplysningene vil være en målsetting for amerikansk myndigheter ihht. FISA Section 702, Executive Order 12333 eller PPD 28.
  - Kryptering og anonymisering kan være en løsning for IaaS og PaaS, men er upraktisk ved bruk av SaaS. Krypteringsnøkler lagret i USA gir ingen beskyttelse, fordi amerikanske myndigheter kan kreve disse utlevert. Admin-tilgang fra USA betyr overføring selv om data er lagret i EU/EØS.
- Veileder fra Datatilsynet:

  https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/

Art. 83: Generelle vilkår for ilegging av overtredelsesgebyr

1. *Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr gjøres i henhold til denne artikkel for overtredelser av GDPR.*
2. *Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om gebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til bl.a.:*
   a) *karakteren, alvorlighet og varigheten av overtredelsen, idet det tas hensyn til behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,*
   b) *hvorvidt overtredelsen ble begått forsettlig eller uaktsom.*
4. *Ved mindre overtredelser kan det ilegges gebyr på opptil 10 000 000 euro eller, dersom det dreier seg om et foretak, på opptil 2% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes.*
5. Ved alvorlige overtredelser kan det ilegges gebyr på opptil 20 000 000 euro eller, dersom det dreier seg om et foretak, på opptil 4% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes:


Vurdering av personvernkonsekvenser (DPIA)
Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Ansvarsforhold
Informasjonssikkerhet
Personvernprinsipper
Rettslig grunnlag
Nødvendighet og proporsjonalitet
Rettigheter
Friheter
Plikter for alle
Tilleggsplikter for DPIA
Sammenstilling og presentasjon av funn
Ledelsens validering av DPIA
Hensynet til interessenter
Gjennomgang, beslutning og godkjenning
Apenhet
Forutsigbarhet
Risiko for de registrertes rettigheter og friheter
Medbestemmelse
Tillit
Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 35 i EUs personvernforordning (GDPR)
Datatilsynet

Art. 35: Vurdering av personvernkonsekvens (DPIA)

1. *I tilfelle behandlingen vil medføre høy risiko for fysiske personers personvernrettigheter og -friheter, skal den behandlingsansvarlig foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (foreta en DPIA).*
2. *Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er oppnevnt, for gjennomføring av en DPIA.*
3. *DPIA er særlig nødvendig i følgende tilfeller:*
   a. *systematisk og omfattende behandling av persondata,*
   b. *behandling av særlige kategorier av opplysninger eller av personopplysninger om straffedommer og lovovertredelser,*
   c. *systematisk overvåking i stor skala av et offentlig område.*

Det som menes med **«rettigheter og friheter»** er først og fremst rettighetene som beskrives i GDPR Art.12 – 22, men også rettigheter nedfelt i Grunnloven, FNs menneskerettigheter og Den europeiske menneskerettighetskonvensjonen som bl.a. beskriver retten til privatliv, kommunikasjonsvern, ytringsfrihet, religionsfrihet, retten til å organisere seg, og frihet fra diskriminering.

To typer personvernrisiko

Hvem er trusselaktøren?

Trusselaktører:

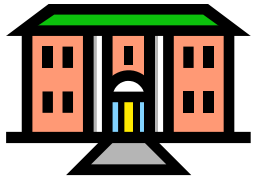
- script kids
- hacktivisme
- organisert kriminalitet
- terrorisme
- statlige cyberoperasjoner

Trusler er f.eks.:

- brudd på KIT for personopplysninger
- tyveri og publisering av personopplysninger

→ Risikovurdering ifølge Art. 32.

Trusselaktører:



- den behandlingsansvarlige
- databehandleren

Trusler er f.eks:

- uønsket innsamling
- urettmessig diskriminering
- re-identifisering
- lagring lenger enn nødvendig

→ DPIA ifølge Art. 35.

Sikkerhetsrisikovurdering er ikke DPIA!

- Art.32 relaterer risikovurdering til personopplysningssikkerhet for behandlingen (ikke DPIA)
  - gjennomføres før behandlinger, oppdateres regelmessig og ved endringer
  - skal identifisere områder som kan medføre utilsiktet eller uautorisert tilgang, endring, sletting, tap eller utlevering av personopplysninger
  - skal skaffe kunnskap om hvilke risikoer som eksisterer
    - er nødvendig for å kunne iverksette tilstrekkelig sikkerhetstiltak
- Art.35 relaterer risikovurdering til personvernkonsekvens (DPIA)
  - gjennomføres for behandlingsaktiviteter som sannsynligvis vil medføre en høy risiko for rettigheter og friheter
    - hensikten er å håndtere en risiko i inngripende behandlinger som medfører økt fare for å krenke fysiske personers rettigheter og friheter. Sikkerhetstiltak vil ikke nødvendigvis redusere denne faren, og risikoreduserende tiltak må fokusere på hvordan behandlingen utføres og hvordan rettighetene ivaretas.

Når må man gjennomføre en DPIA

*«Dersom det er **sannsynlig** at en **type behandling**, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (Art. 35.1)

- Vurderingen er obligatorisk når behandlingen **sannsynligvis** vil medføre en høy risiko. Ved uvisshet om det er nødvendig å gjennomføre en DPIA, anbefales å gjøre det likevel, som et nyttig verktøy for at behandlingsansvarlig får visshet om at de overholder personvernforordningen.

Art

Behandlingens iboende karakteristikk:

- Vanskelig å utøve sine rettigheter
- Uforutsigbarhet, liten åpenhet og uvisshet om ivaretakelse av prinsipper
- Systematisk behandling
- Særlige kategorier
- Skjevt maktforhold
- Ny teknologi

Omfang

Behandlingens størrelse/rekkevidde:
Er stort omfang det samme som stor skala?

- Antall registrerte involvert (tall eller %)
- Volumet av data (antall variabler, detaljer)
- Lagringstid (kort, tidsavgrenset, permanent)
- Geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt, globalt

Formål

Hva skal personopplysningene brukes til:

- Kontrollformål
- Behandling for å ta beslutninger som får betydning for den registrerte
- Å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personopplysninger

Sammenheng

Hvilken forventning om personvern omgir den konkrete behandlingen:

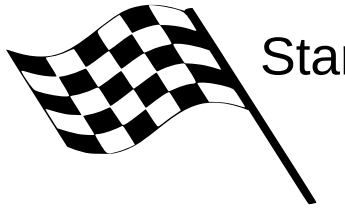
- Forventning om konfidensialitet (helse, velferd, arbeidsforhold)
- Forventning om privatliv (hjem, rekreasjon)
- Behandling av personopplysninger fra ulike datasett som er innsamlet for ulike forhold

Absolutt nødvendighet av DPIA

- DPIA er absolutt nødvendig i følgende tilfeller:
  - systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
  - behandling av særlige kategorier av personopplysninger i stor skala
  - Systematisk overvåking av offentlig område i stor skala
- Datatilsynet **må** publisere liste over når det er påkrevd
- Datatilsynet *kan* publisere liste over når det ikke er påkrevd

Art. 35 (3-5)

Prosess rundt DPIA



Start

Sannsynlighet for høy risiko? Art. 35(1),(3),(4)

JA

NEI

Unntak? Art. 35(5),(10)

JA

NEI

Ikke krav om DPIA, behandlingen kan begynne

Atferdsnormer Art. 35(8)

(codes of conduct)

Råd fra PVO Art. 35(2) PVO kontrollerer gjennomføringen Art. 39(1c)

Innhente synspunkter fra de registrerte Art. 35(9)

DPIA Art. 35(7)

Revidering ved behov, Art. 35(11)

Høy restrisiko? Art 36(1)

JA

NEI

Forhåndsdrøftelse med Datatilsynet

Behandlingen kan begynne

Deltagere i DPIA

- Den behandlingsansvarlige:
  - Selve arbeidet kan delegeres til andre, men den behandlingsansvarlige står til regnskap for at behandlingen er lovlig

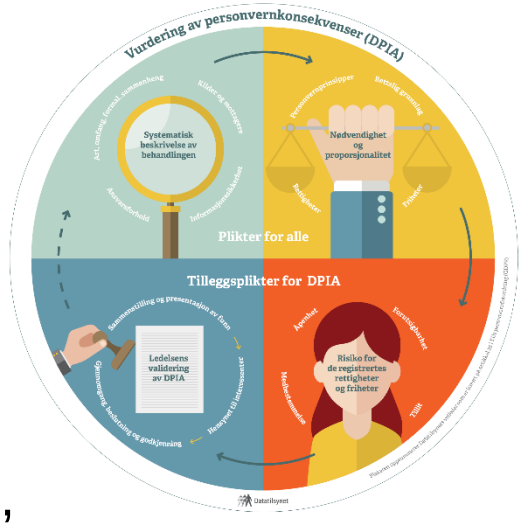
- Deltagere
  - **Personvernombudet**
  - **Databehandlere**
  - **Behandlingsansvarlig** må hente inn synspunktene fra **de registrerte** eller deres representanter dersom dette er relevant
  - God praksis: involvere relevante aktører og eventuelt eksperter på området
  - CISO og PVO kan anbefale at en DPIA gjennomføres, og bidra i prosessen

Planlegging av DPIA

- Forutsetning: Behandlingen må være lovlig og oppfylle grunnkrav som følger av forordningens øvrige bestemmelser
  - En DPIA må gjennomføres forut for behandlingen, og bør startes så tidlig som mulig.
  - Det er en kontinuerlig prosess, ikke en engangsforeteelse .

- Følg god praksis:
  - Definer og dokumenter roller og ansvarsområder.
  - Dokumenter hvorfor dere eventuelt gjennomfører en behandling i strid med de registrertes synspunkter.
  - Dokumenter hvorfor dere eventuelt ikke ber om den registrertes synspunkter i det hele tatt.

Hovedelementer i DPIA



Trinn i DPIA-prosessen:

1. «Lag en systematisk beskrivelse av den planlagte behandlingen og formålet med behandlingen»,
2. «Foreta en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene»,
3. «Gjør en vurdering av risikoene for de registrertes rettigheter og friheter»,
4. «Spesifiser de planlagte tiltakene»:
   - «for å håndtere risikoene»,
   - «for å påvise at Personvernforordning overholdes».
5. Få ledelsens validering av DPIA.

I praksis vil DPIA-teamet først lage et utkast til systematisk beskrivelse, deretter gjøre en iterasjon over punktene 2 – 4 til det vurderes at "behandling ikke får konsekvenser for den registrertes rettigheter og friheter", og til slutt redigere endelig versjon av den systematiske beskrivelsen, som valideres av ledelsen.

Art. 35 (7)

Systematisk beskrivelse av behandlingen

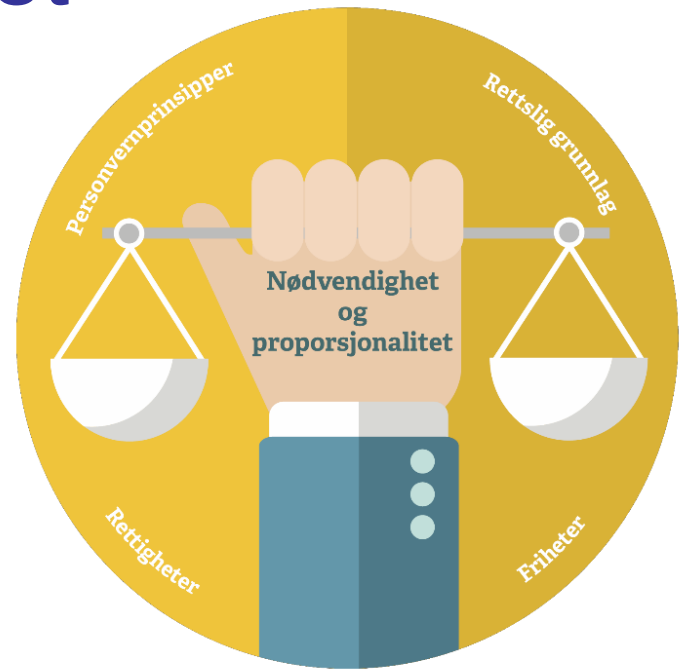
- Gjennomgå og kvalitetssjekk oversikt og beskrivelse av behandlingen
  - Behandlingens art, omfang, formål og sammenhengen behandlingen utføres i
  - Mottakere, dataflyt og lagring
  - Funksjonell beskrivelse av behandlingen og alle aktiva
  - Aktuelle referanser for behandlingen er dokumentert.

- **Mål:** Den behandlingsansvarlig har en fullstendig oversikt over behandlingen, og gjør en **kvalitetssjekk** på at beskrivelsene som er gjort er komplette og tydelige.

Art. 35 (7.a)

Nødvendighet og proporsjonalitet

- Behandlingsgrunnlag
- Overføringsgrunnlag
- Formål(ene)
- Dataminimering
- Riktighet
- Lagringsbegrensning
- De registrertes rettigheter
- De registrertes friheter



Kontroller om det er nødvendig eller mulig å forbedre måten man ivaretar personvernprinsippene, og de registrertes rettigheter og friheter. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.

Mål: I denne fasen **kvalitetssikres** det at valgene er legitime og utført for å bidra til at behandlingen er nødvendig og står i et rimelig forhold til formål, for å etterleve lovkravene

Art. 35 (7.b)

Vurdering av konsekvens og planlagte tiltak

- Vurdering av risiko for brudd på rettigheter og friheter
  - Manglende nødvendighet og proporsjonalitet
  - Manglende reell medbestemmelse
  - Manglende reell åpenhet
  - Manglende forutsigbarhet

1. Identifiser trusler
2. Avklar potensielle konsekvenser
3. Anslå sannsynlighet for at en hendelse oppstår
4. Anslå alvorlighetsgrad for hver risiko
5. Bestem tiltak for å håndtere risikoene

- **Mål: Ha en behandling som ikke får konsekvenser for den registrertes rettigheter og friheter.**

Art. 35 (7.c-d)

Hvordan vurdere personvernkonsekvens?

- Vurdere sannsynligheten for, og konsekvensen av at (ikke uttømmende liste!):
  - personopplysninger behandles uten rettslig grunnlag
  - personopplysninger behandles på en ikke rettferdig måte
  - det mangler åpenhet rundt behandlingen av personopplysninger
  - det samles inn mer personopplysninger enn nødvendig for formålet
  - personopplysninger som behandles er ikke korrekte
  - personopplysninger lagres lengre enn nødvendig for formålet
  - den registrerte mangler informasjon til å gjøre et informert valg
  - den registrerte ikke får innsyn i lagrede personopplysninger
  - den registrerte ikke får korrigert eller slettet sine personopplysninger
  - det ikke er lagt til rette for dataportabilitet
  - de registrertes rettigheter ikke ivaretas ved profilering
  - behandlingen kan resultere i diskriminering
  - behandlingen begrenser ytringsfrihet og religionsfrihet

Eksempler på personvernstiltak

- Samle inn mindre personinformasjon
- Redusert behandling av personinformasjon
- Tillatt rett til reservasjon
- Løpende informasjon, flere kanaler
- Særskilt tilrettelagt innsynsportal
- Automatisk sletting
- Anonymisering
- Forklarlig AI
- Alternativ manuell prosedyre for beslutning

Ledelsens validering av DPIA

- Forutsetninger som ledelsen MÅ kjenne til:
  - Virksomheten har en behandling som sannsynligvis kan medføre høy risiko for den registrertes rettigheter og friheter, og er omfattet av artikkel 35.
  - Må få forståelse av den gjennomførte DPIA, identifiserte risiko og tiltak.
  - Å ikke gjøre DPIA, utføre DPIA feil, eller ikke rådføre seg med korrekte instanser kan innebære administrative bøter

- Forberede dokumentasjon for ledelsens validering
  - Sammenstill og presenter funn
  - Dokumenter hensynet til interessenter
  - Ledelsens gjennomgang, beslutning og godkjenning

Ledelsens beslutning om DPIA

- Ledelsen beslutter og begrunner om DPIA er:
  - Godkjent/validert => Behandling kan starte opp.
  - Betinget av forbedringer (forklar på hvilken måte) => Revidert DPIA skal fremlegges på nytt for ledelsen.
  - Avvist: Virksomheten beslutter å ikke gjennomføre behandlingen.

- Når DPIA er
  - behandlet i ledergruppen mer enn én gang, og
  - risikoen fremdeles er høy og viljen til å behandle data fremdeles er stor

=> Nødvendig å anmode om forhåndsdrøftelse med Datatilsynet.

- Virksomheten må dokumentere at risikoen ikke kan reduseres.
- Beslutning om å be om forhåndsdrøftelse skal tas av ledelsen.

Forhåndsdrøftelse med Datatilsynet

- Ved høy risiko, som ikke kan reduseres, skal Datatilsynet involveres i forhåndsdrøftelser.
- Det stilles krav til dokumentasjon som skal sendes inn, og at behandlingsansvarlige har fulgt Datatilsynets veiledning.
- Maksimum behandlingstid hos Datatilsynet er 8 (+ 6) uker.
- En skriftlig, formalisert prosess som skal vurdere:
  - om behandlingen skjer i tråd med personvernforordningen, ivaretar personvernprinsippene, de registrertes rettigheter og friheter
  - om den behandlingsansvarlige i tilstrekkelig grad har identifisert risikoen
  - om risikoen i tilstrekkelig grad er redusert
- MÅL: unngå behandling av personopplysninger som medfører høy risiko for de registrertes rettigheter og friheter

Referanser

Veiledere fra Datatilsynet:

- Gjennomføring av DPIA

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

- Virksomhetenes plikter ifm. GDPR

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

- Programvareutvikling med innebygd personvern

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

- Veileder om overføring til USA:

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/privacy-shield-avtalen-mellom-usa-og-eueos-er-opphevet/

Slutt på presentasjonen