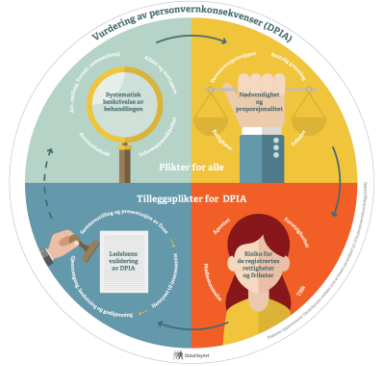
Sikkerhetsrisikovurdering og personvernkonsekvensvurdering - ulikheter og likheter

Veronica Jarnskjold Buer | Avdelingsdirektør for Teknologi, Analyse og sikkerhet, Datatilsynet

30.August 2023

Datatilsynet

VS.



Artikkel 32

Artikkel 35

Vurdering av sikkerheten ved behandling av mine opplysninger.

ROS – hvor godt sikrer virksomheten mine opplysninger mht. K-I-T-R

Vurdering av hvor inngripende behandlingen er for meg.

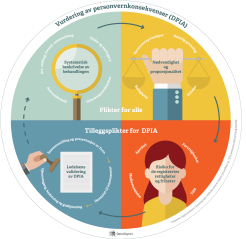
Hvor forutsigbar er behandlingen, hvor stor medbestemmelse har jeg av mine opplysninger i behandlingen, hvor stor åpenhet er det om behandlingen gitt personvernprinsippene, mine rettigheter, friheter og personvern.

Datatilsynet

Eksempler på likheter og ulikheter

- Artikkel 32
  - Gjennomføres alltid
  - Ta hensyn til art, omfang formål og sammenheng
  - Tar virksomheten perspektiv
  - Identifiserer risiko og implementere tiltak (herunder identifisere verdier og trusler)
  - Formål med ROS: Sikkerhet ved behandlingen, og implementere tilstrekkelig sikkerhetstiltak med hensyn til risiko
  - Inkluderer Konfidensialitet, Integritet, Tilgjengelighet og Robusthet.
  - Tiltakene må ta hensyn til Stat-of-the-art og gjennomføringskostnadene
  - Både organisatoriske og tekniske tiltak

- Artikkel 35
  - Gjennomføres når det er sannsynlig at behandlingen kan medføre høy risiko høy for den registrertes rettigheter og friheter
  - Ta hensyn til art, omfang formål og sammenheng
  - Tar den registrertes perspektiv
  - Identifiserer risiko og implementere tiltak (herunder identifisere verdier og trusler)
  - Formål med vurdering av personvernkonsekvenser: vurdere om behandlingen er for inngripende og hvilke konsekvenser det vil få for personopplysningsvernet, og den registrertes reelle medbestemmelse, reelle åpenhet og forutsigbarhet med behandling
  - Inkluderer forholdsmessighet og nødvendighet
  - Tiltak kan være krav om fornyet samtykke, rett til reservasjon, løpende informasjon i flere kanaler, særskilt tilrettelagt innsynsportal, krav til automatisk sletting/anonymisering, sikkerhetstiltak



Regelmessig repetisjon

Regelmessig repetisjon

Risikovurdering Artikkel 24, 25, 32 "... risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter ved behandling"

Hvis "det sannsynlig ... vil medføre en høy risiko for fysiske personers rettigheter og friheter"

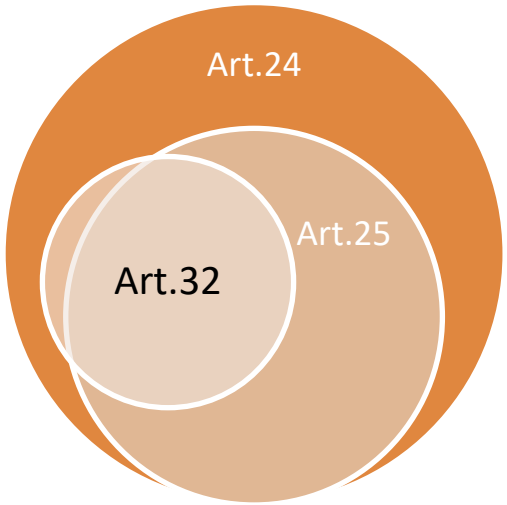
Art. 35 DPIA

Rettigheter og friheter

- Lovlighet, rettferdighet, åpenhet
- Formåls-begrensing
- Data-minimering
- Riktighet
- Lagrings-begrensning
- Integritet og konfidensialitet

Tiltak og garantier for samsvar og risiko-håndtering

Tiltak og garantier



Art.24: Behandlings-ansvarlig implementerer tilstrekkelige tiltak

Art.25: Tiltak og garantier er innebygd i behandlingen + strengt nødvendig behandling er standard

Art.32: Tiltak for å sikre personopplysninger (også for databehandlerne)

Ansvarlighet

Når ?

- Art 35(3)
- WP29-Gruppens kriterier
- Datatilsynets *må*-liste
- Art 35 (10)/Art 36(4)

Kvalitetssikring av allerede gjennomført arbeid:

- med systematisk beskrivelse av behandlingen
- ved Nødvendighet & Proporsjonal

Behandlingens art, omfang, formål og sammenheng

Art

Behandlingens iboende karakteristikk:

- Vanskelig å utøve sine rettigheter
- Uforutsigbarhet, liten åpenhet og usikkerhet om ivaretakelse av prinsipper
- Systematisk behandling
- Særlige kategorier
- Skjevt maktforhold
- Ny teknologi / gammel teknologi brukt på ny måte
- Kompleksitet
- Automatiske avgjørelser

Omfang

Behandlingens størrelse/rekkevidde:

- 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 med mål om 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
- Kjeden av aktiviteter i behandling
- Deling med andre behandlingsansvarlige eller virksomheter

Eksempel fra vurdering av side på FB…

Risiko knyttet til behandlingens art:

- Det er vanskelig for den registrerte å utøve sine rettigheter overfor Facebook
- Behandlingen av personopplysninger er uforutsigbar
- Behandlingen av personopplysninger er preget av mangel på åpenhet overfor den registrerte
- Usikkerheter rundt ivaretakelsen av flere personvernprinsipper
- Systematisk behandling i form av profilering og automatiske avgjørelser
- Hvorvidt det er et skjevt maktforhold til brukeren kan problematiseres
- Bruk av innovativ teknologi er i stadig endring

Risiko knyttet til behandlingens formål:

- Facebook sine formål er vage, uklare og omfattende, samt at de divergerer i høy grad fra våre formål for behandling.
- Det er usikkerhet om hvorvidt personopplysningene vil brukes til nye eller andre formål.
- Beslutningene som tas om den registrerte kan få betydelig betydning for den registrerte
- Det treffes beslutninger om den registrerte basert på systematisk og omfattende analyse av personopplysninger

Risiko knyttet til behandlingens omfang:

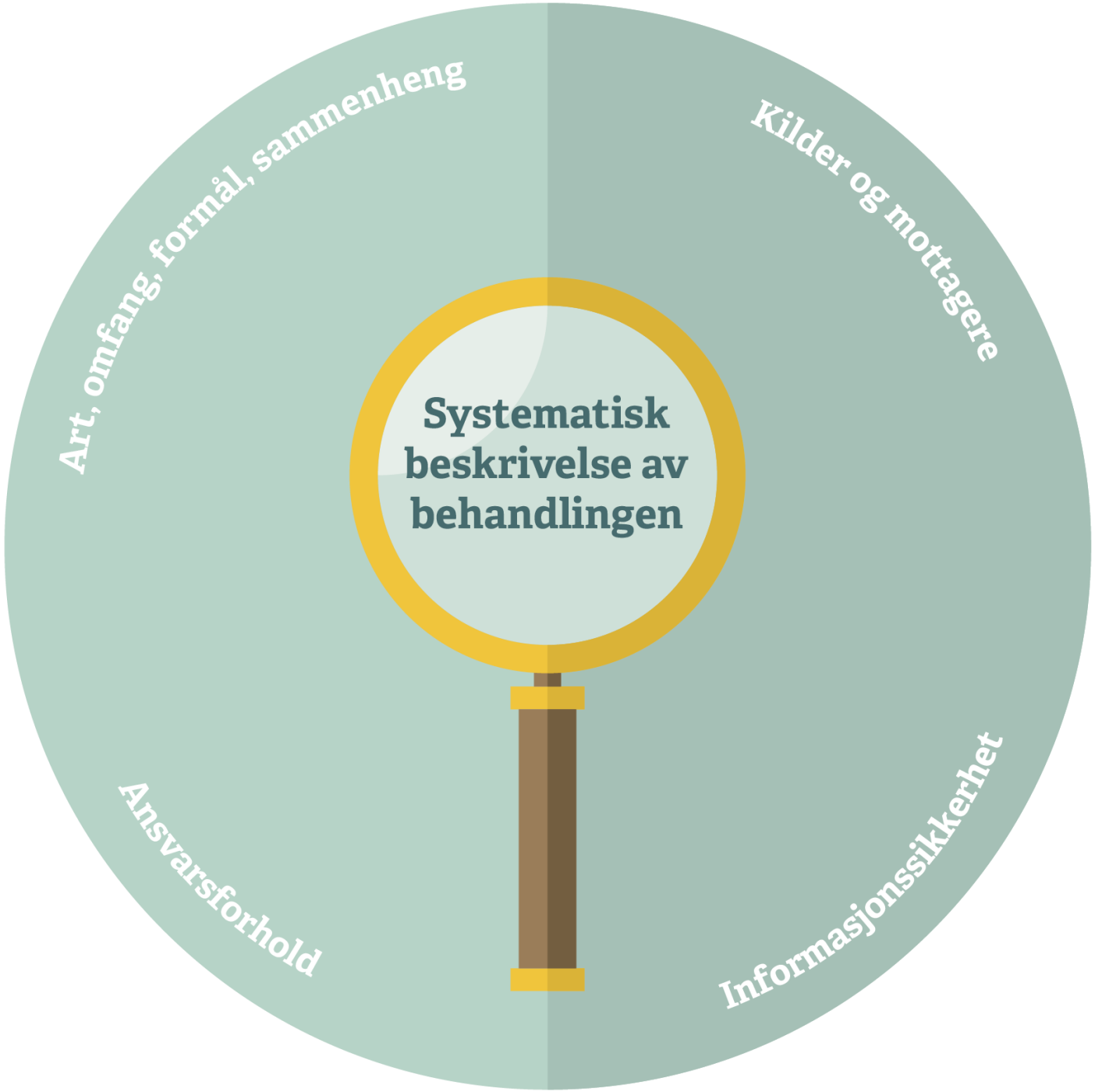
- Behandlingen vil innebære en rekke kategorier personopplysninger, herunder særskilte kategorier data.
- Behandlingen vil potensielt innebære behandling av personopplysninger om sårbare personer
- Behandlingen vil innebærer et høyt antall registrerte.
- Volumet av personopplysninger om den registrerte er stort og detaljert
- Vi mener det er usikkerheter rundt lagringstid, som potensielt er permanent.
- Det geografiske omfanget på lagring er globalt, det vil si også utenfor EU/EØS.

Risiko knyttet til behandlingens sammenheng:

- Vi mener det er usikkerhet rundt kilder, datasett og sammenstilling av forskjellige datasett på og utenfor plattformen
- Vi mener den registrerte vil kunne ha en forventning om konfidensialitet og privatliv i visse typer kommunikasjon med en side på plattformen.
- Vi mener det er vanskelig for den registrerte å ha oversikt og kontroll over egne opplysninger.
- Vi mener dataflyten og kjeden av behandlinger er uklar, inkludert hvem som er mottakere av personopplysninger

Høy risiko

Begrunnelse for gjennomføre DPIA mht page på FB = risiko høy for den registrertes rettigheter og friheter	**Art:** Vanskelig for den registrerte å utøve sine rettigheter, behandlingene er **uforutsigbarhet,** behandlingen har liten åpenhet og usikkerhet om ivaretakelse av personvernprinsippene, systematisk behandling, særlige kategorier personopplysninger, skjevt maktforhold, Kompleksitet rundt og i behandlingen, det gjøres profilereing og foretas automatiserte avgjørelser, (Ny teknologi / gammel teknologi brukt på ny måte?) **Omfang:** Behandlingens størrelse/rekkevidde er geografisk **global** og antall involverte har ingen begrensning, kan i prinsippet omfatte mer enn 2 milliarder. Volumet av personopplysninger knyttet til enkeltindivider er stort og detlajert. Lagringstid er som utgangspunkt permanent, og usikkerhet om personopplysninger blir slettet etter sletting. **Formål:** Personopplysningene skal brukes til å ta beslutninger som får betydning for den registrerte og treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personopplysninger. **Sammenheng:** Den registrertes har i visse typer korrespondanse på plattformen en forventning om konfidensialitet og privatliv. Datasett fra ulike behandlingsansvarlige og innsamlet for ulike forhold sammenkobles. Kjeden av aktiviteter i behandlingen er utklar og uviss, det samme gjelder også for deling av personopplysninger med andre behandlingsansvarlige eller virksomheter

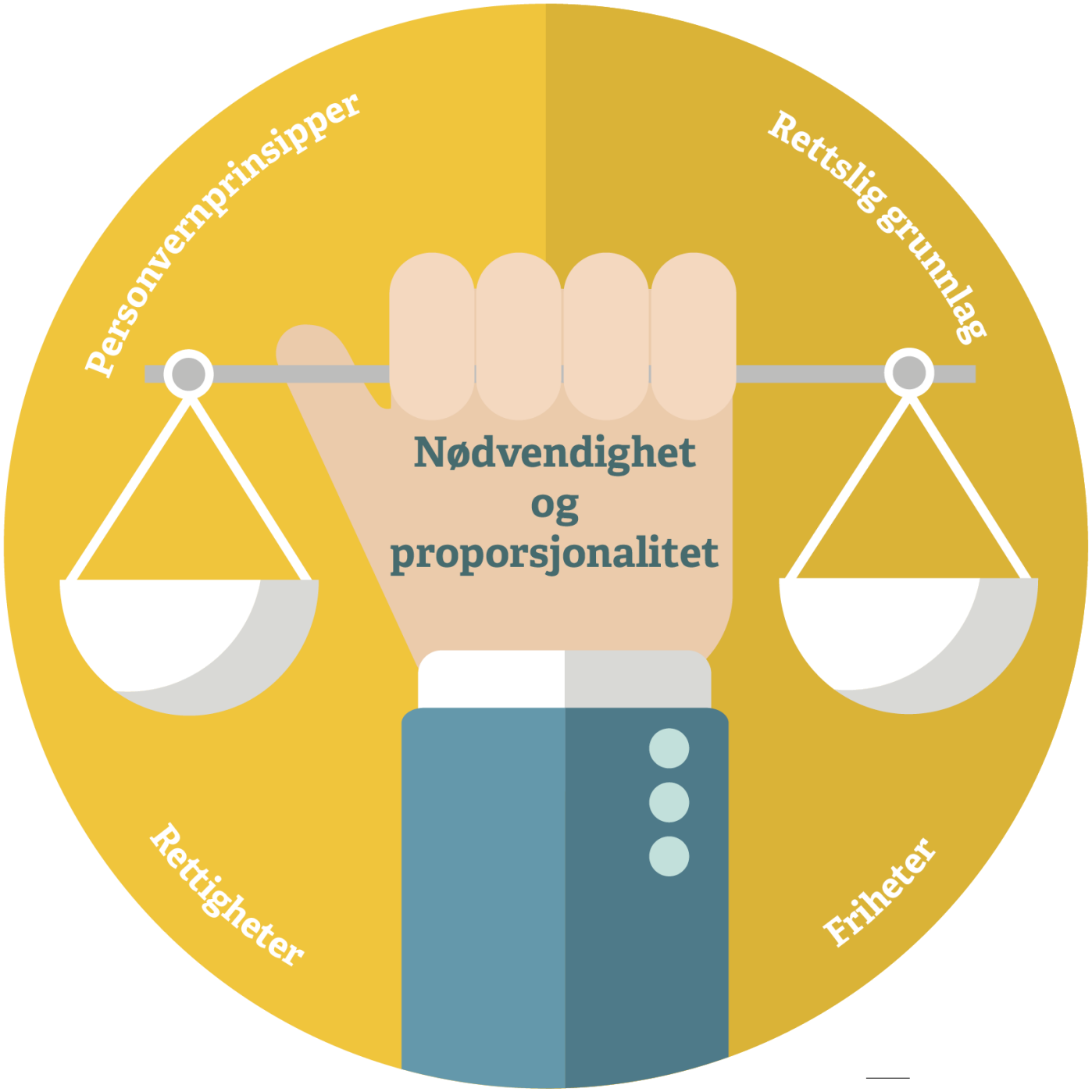


Mål:
Denne fasen skal bidra til at den behandlingsansvarliges får en fullstendig, tydelig og komplett oversikt (beskrivelse) over behandlingen inkl. teknologi, dataflyt, teknologi og ansvarsforhold.

Behandlingsoversikt

- Behandlingens art, omfang, formål og sammenheng
- Hvilken sammenheng behandlingen utføres i (kontekst)
- Kilder, mottagere, informasjonssikkerhet og ansvarsforhold

1	Behandlingsoversikt	Offentlig informasjon (behandlet av datatilsynet)	Kommunikasjon med bruker (behandlet av datatilsynet)	Delt behandlingsansvar, DT og FB, artikkel 26	Facebook brukerdata (behandlet av facebook)
18				**Behandlingens formål**	
19	Hva er formålet med behandlingen?	Informasjon om DTs kjernevirksomhet og veiledning i personopplysningsloven og nærliggende områder. Spredning til nye målgrupper (særlig privatpersoner og små virksomheter som vi sliter med å nå ut til via andre kanaler), økt synlighet til innholdet vårt, skape debatt om personvern og nærliggende tema. Øke bevisstheten om personvern, regler og rettigheter i befolkningen.	Informasjon om DTs kjernevirksomhet og veiledning i personopplysningsloven og nærliggende områder. Spredning til nye målgrupper (særlig privatpersoner og små virksomheter som vi sliter med å nå ut til via andre kanaler), økt synlighet til innholdet vårt, skape debatt om personvern og nørliggende tema. Øke bevisstheten om personvern, regler og rettigheter i befolkningen. (ikke saksbehandling eller individuell veiledning).	Formålet mellom DT og FB spriker. FBs angivelse av formål er omfattende og vag, og oppfyller neppe kravet til at formål skal være spesifikke.	Facebook behandler en mengde ulike personopplysninger. Det er derfor flere formål: 1) Å tilby tilpassede tjenester samt forbedre dem 2) Utføre målinger og analyse for å støtte behovene til sine samarbeidspartnere (slik som annonsører). 3) Fremme sikkerhet for å detektere og bekjempe uønsket materiale. Dette er for å opprettholde produktenes integritet. 4) Kommunisere med sine brukere 5) Bistå og støtte forskning og innovasjon
20	Vil det være kontrollformål	Nei	Nei		**Nei**
	Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?	Nei	Nei	Ja. Datatilsynet og FB har ulik tilnærming.	Ja Facebook gjør analyse av personopplysninger for å oppnå formålene som er beskrevet Data Policy. Utdrag:"To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide where you have given your explicit consent); how you



Mål:
I denne fasen sørge for at den behandlingsansvarliges valg er **legitime** og utført for å bidra til at behandlingen er **nødvendig** og står i et **rimelig** forhold til formålene.

Nødvendighet og proporsjonalitet

	Nødvendighet og proposjonalitet	Offentlig informasjon (behandlet av datatilsynet)	Interaksjon med brukere (behandlet av datatilsynet)	Delta FB og DT	Facebook brukerdata (behandlet av face
2				**Behandlingsgrunnlag:**	
3	Behandlingsaktiviteter For eksempel, lagring, deling, utlevering, analyse osv.	Registrerer, lagrer, deler, analyserer, sletter, redigerer.	Registrerer, lagrer, deler, analyserer, sletter, redigerer, sammenstiller.	Registrerer, lagrer, deler, analyserer, sletter, redigerer, sammenstiller, profilerer, annonserer.	Lagring, deling, analyse, utlevering, annonser (https://www.facebook.com/policy.php)
6	Er det skilt mellom hva som er nødvendig for avtale og hva som skal baseres på samtykke?	N/A	N/A	Tvilsomt å basere all behandling på avtale. EDPBs utkast til veiledning om nødvendig for avtale, nr 2/2019.	Ja. Se Celle 4 E. https://www.facebook.com/about/privacy/le
7	Hvordan ivaretas åpenhet i behandlingen?	Datatilsynet ønsker og vil tilstrebe full åpenhet om egen behandling av personopplysninger. DT ivaretar åpenhet ved å gi informasjon om vår behandling av personopplysninger via FB både på FB og på vår hjemmeside, slik at man ikke må ta i	Datatilsynet ønsker og vil tilstrebe full åpenhet om egen behandling av personopplysninger. DT ivaretar åpenhet ved å gi informasjon om vår behandling av personopplysninger via FB både på FB og på vår hjemmeside, slik at man ikke må ta i	Se kolonne C for DT og kolonne E for FB. Datatilsynet mener det er problematisk for åpenheten at FBs informasjon er vanskelig tilgjengelig, og at formålene er lite spesifikke, og at ikke all type behandling er forklart eller dokumentert fra FBs side	Offentlig tilgjenglig informasjon følgende ste lenkene under, samt muligheter til å se anno andre med dine data. Enkelt å hente ut egne https://www.facebook.com/about/privacy/le https://www.facebook.com/policy.php https://www.facebook.com/ads/preferences
8				**Formål(ene):**	
9	Er formålet klart definert? Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget (artikkel 5.1 b).	Ja. Se rad 19 i fane Behandlingsoversikt.	Ja. Se rad 19 i fane Behandlingsoversikt.	For DT: Ja, se rad 19 i fane Behandlingsoversikt. For FB: Vi mener DT er lite spesifikke og altomfattende og uklare.	Nei.
	Er formålet definert slik at det samsvarer med forventningene til de registrerte?	Ja	Ja	For DT: Ja. For FB: Vi mener DT er lite spesifikke og altomfattende og uklare. KRITISK, HHH	Nei. Det er likevel enkeltfunksjoner i facebook so tvers av formål. Eksempelvis kan man oppgi telefonnummer med det formål om å gjenop passord dersom det skulle være nødvendig el

Den registrertes perspektiv
Verdiene som skal beskyttes er personopplysningene.

Håndtere risiko i inngripende behandlinger som medfører økt fare for å krenke fysiske personers rettigheter og friheter.

For å oppnå tillit til behandlingen må man sørge for reell åpenhet, forutsigbarhet og medbestemmelse.

Risiko for den registrertes rettigheter og friheter

- Manglende reell
- Manglende foru
  den registrerte v
- Manglende åper
- Avklar potensiel
  personopplysnir
  sårbarheter og d
- Tiltak

Vurdeing av behandlingen fra den registretes perspektiv	Offentlig informasjon (behandlet av datatilsynet)	Interaksjon med brukere (behandlet av datatilsynet)	Delta
Manglende reell medbestemmelse - den registrerte har et valg,			
Kartlegging om den registrertes reelle medbestemmelse			
Trusler ved manglende reell medbestemmelse for den registrerte			
Alvorlighetsgrad: hvor alvorlig er det at den reg. ikke har reell medbestemmelse			
Konsekvenser dersom den reg. har manglende har reell medbestemmelse			
Sannsynlighet for at konsekvensene inntreffer			
Tiltak for å at den registrerte skal ha en reell medbestemmelse			
Restrisiko for den registrertes rettigheter og friheter etter implementert tiltak			
Manglende reell åpenhet - virksomheten evner ikke å forklare komplekse behandlinger eller forventet res			
Kartlegge om den behandlingansvarige er åpen overfor den registrerte om reell behandling av personopplysninger			

Den behandlingsansvarlige ansvar:

- Påvise at Artikkel 5 (1) overholdes.
- Gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordning. Regelmessig vurdere oppdatering. Artikkel 24 (1).


SLANE
ca.nz
DEN EGENTLIGE HENSIKTEN MED URINTESTINGEN ER VEL Å NEDVERDIGE VÅRE ANSATTE?
CHRIS

Takk for oppmerksomheten!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

@datatilsynet (Twitter)
@veronica_buer