Hva betyr GDPR for forskere

Livet etter GDPR

Camilla Nervik

Seniorrådgiver, Datatilsynet

Hva betyr GDPR for forskere?

Livet med GDPR

Camilla Nervik

Seniorrådgiver, Datatilsynet

Hva betyr GDPR for forskere?

Livet med

personvernforordningen
og ny personopplysningslov
og norsk særlovgivning

Camilla Nervik

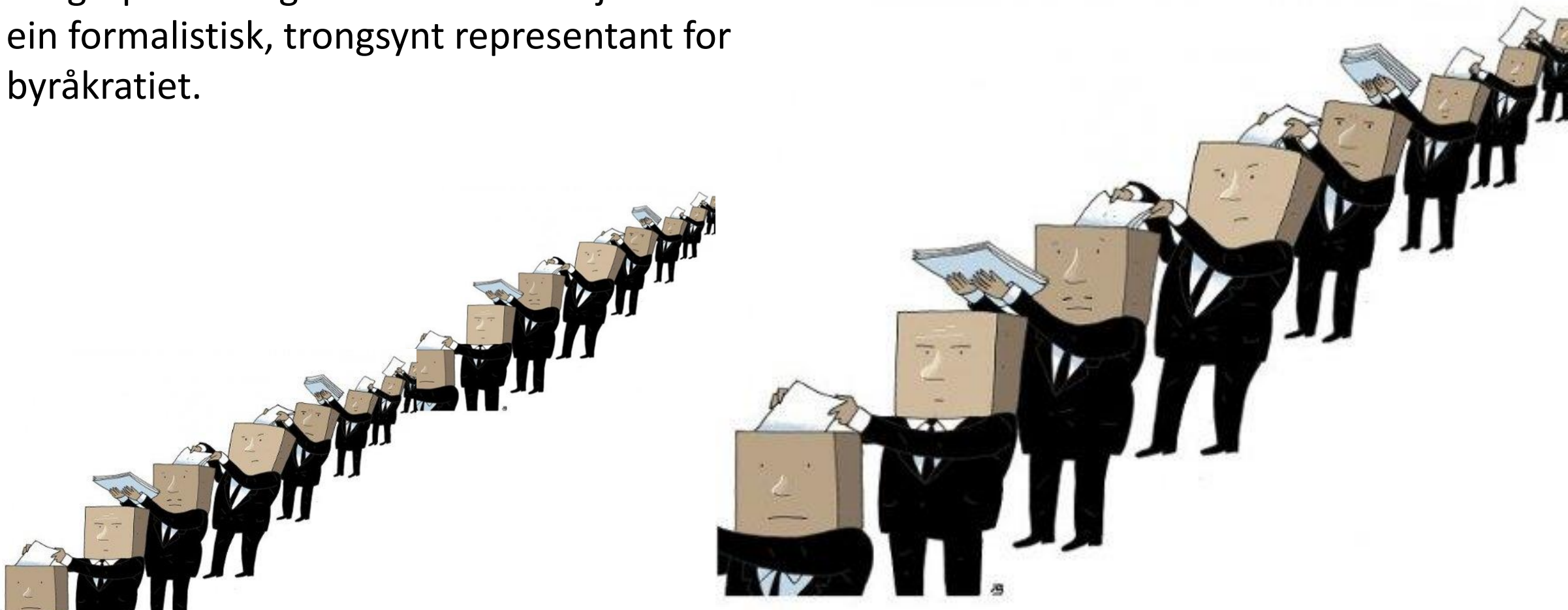
Seniorrådgiver, Datatilsynet

Tema for halvtimen

- Kort og enkelt om forskjellene – byråkratiet
- Hva med de tillatelsene som eksisterer?
- Hva må man gjøre fremover når man skal forske?
  - Vurdering av personvernprinsippene
  - Vurdering av rettslig grunnlag
    - Hvordan involvere personvernombudet?
  - Finnes det et relevant unntak fra forbudet i artikkel 9?
  - Innebygget personvern, DPIA og forhåndsdrøftelser

Byråkrat (uttale byråkrˈat) er ein funksjonær innanfor eit byråkrati eller ein tenesteperson i det offentlege.

Omgrepet kan også brukast nedsetjande om ein formalistisk, trongsynt representant for byråkratiet.



Artikkel 5 – prinsipper

Lovlig, rettferdig og gjennomsiktig
Respekter de registrertes interesser og forventninger. Informer på en forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til uttrykkelig angitte og legitime formål, og ikke (senere) til uforenlige formål.

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig.

Korrekte og oppdaterte
Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Lagringsbegrensning
Det skal ikke være mulig å identifisere de registrerte lenger enn hva som er nødvendig for formålet.

Integritet og konfidensialitet
Personopplysninger sikres mot uautorisert tilgang og mot tap, ødeleggelse eller skade.

Ansvarlighet
Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, etterlevelse.

Artikkel 6 – Rettslig grunnlag

a) Samtykke
b) Nødvendig for å inngå kontrakt
c) Nødvendig for å oppfylle en rettslig forpliktelse
d) Nødvendig for å verne den registrertes vitale interesser
e) Nødvendig for å utføre en oppgave i offentlighetens interesse eller utøve offentlig myndighet
f) Nødvendig for formål knyttet til rettmessige interesser (interesseavveiing)

Artikkel 9 – særlige kategorier av opplysninger

a) Samtykke
b) Hjemmel i lov eller tariff innenfor arbeids-, trygd- eller sosialrett
c) Nødvendig for å verne den registrertes vitale interesser
d) Politisk, religiøs eller fagforeningsorganisasjon
   + berettigede aktiviteter, nødvendige garantier, medlemmer
e) Den registrerte har selv offentliggjort opplysningene
f) Nødvendig for å gjøre gjeldende eller forsvare et rettskrav
g) Viktige samfunnsinteresser
h) Helsehjelp
i) Folkehelsehensyn
j) Arkiv og historisk forskning

Tillegg: Krav om hjemmel i lov

Artikkel 12-22: rettigheter

Noen kjente:

- Informasjon
- Innsyn
- Korrigering
- Sletting/retten til å bli glemt

Noen nye:

- Begrenset behandling
- Innsigelse
- Dataportabilitet
- Automatiserte avgjørelser
- Særskilte rettigheter for beskyttelse av barns personvern

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)

§ 34. Avgjørelsen av om konsesjon skal gis

Ved avgjørelsen av om konsesjon skal gis, skal det klarlegges om behandlingen av personopplysninger kan volde ulemper for den enkelte som ikke avhjelpes gjennom bestemmelsene i kapitlene II-V og vilkår etter § 35. I så fall må det vurderes om ulempene blir oppveid av hensyn som taler for behandlingen.

§ 35. Vilkår i konsesjon

I konsesjonen skal det vurderes å sette vilkår for behandlingen når slike vilkår er nødvendige for å begrense ulempene behandlingen ellers ville medføre for den registrerte.

Når er risiko høy?

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

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 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

Alltid DPIA - Art. 35 (3)

- 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 - Art. 35 (4)

Datatilsynet *kan* publisere liste over når det ikke er påkrevd – Art. 35 (5)

Kriterier for når DPIA kan bli et krav (WP 29)

1. Evaluering eller poengsetting *(scoring)*
2. Automatiske beslutninger med rettslig eller tilsvarende betydelig virkning
3. Systematisk monitorering
4. Særlige kategorier av personopplysninger eller opplysninger av meget personlig karakter
5. Behandling av personopplysninger i stort omfang
6. Sammenstilling eller kobling av datasett
7. Personopplysninger om sårbare personer
8. Ny teknologi eller bruk av eksisterende teknologi til nye formål
9. Når behandlingen forhindrer en enkeltperson i å bruke en rettighet, en tjeneste eller en kontrakt.

Systematisk beskrivelse

- Art 24
- Art 30
- Art. 32
- Art 40,42

Nødvendig-het og proporsjonalitet

- Art 5
- Art 6, 9
- Art 12-22
- EMK, SP, ØSK

Risiko for de registrertes rettigheter og friheter

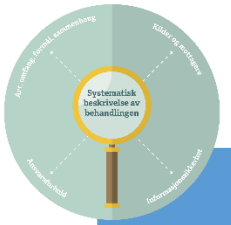
- Medbestemmelse
- Åpenhet
- Forutsigbarhet
- Tillit

Ledelsens validering av DPIA

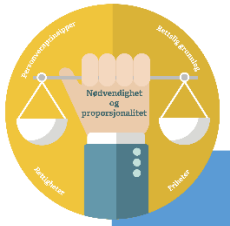
Godkjent/validert

Betinget av forbedringer

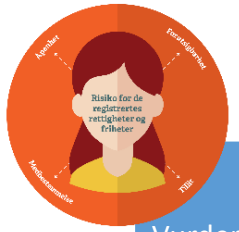
Avvist



- Beskriv personopplysninger (art, omfang, formål og sammenheng)
- Ansvarsforhold (behandlingsansvarlig, databehandlere, underleverandører)
- Kilder, aktiva, mottakere, dataflyt og lagring
- Informasjonssikkerhet



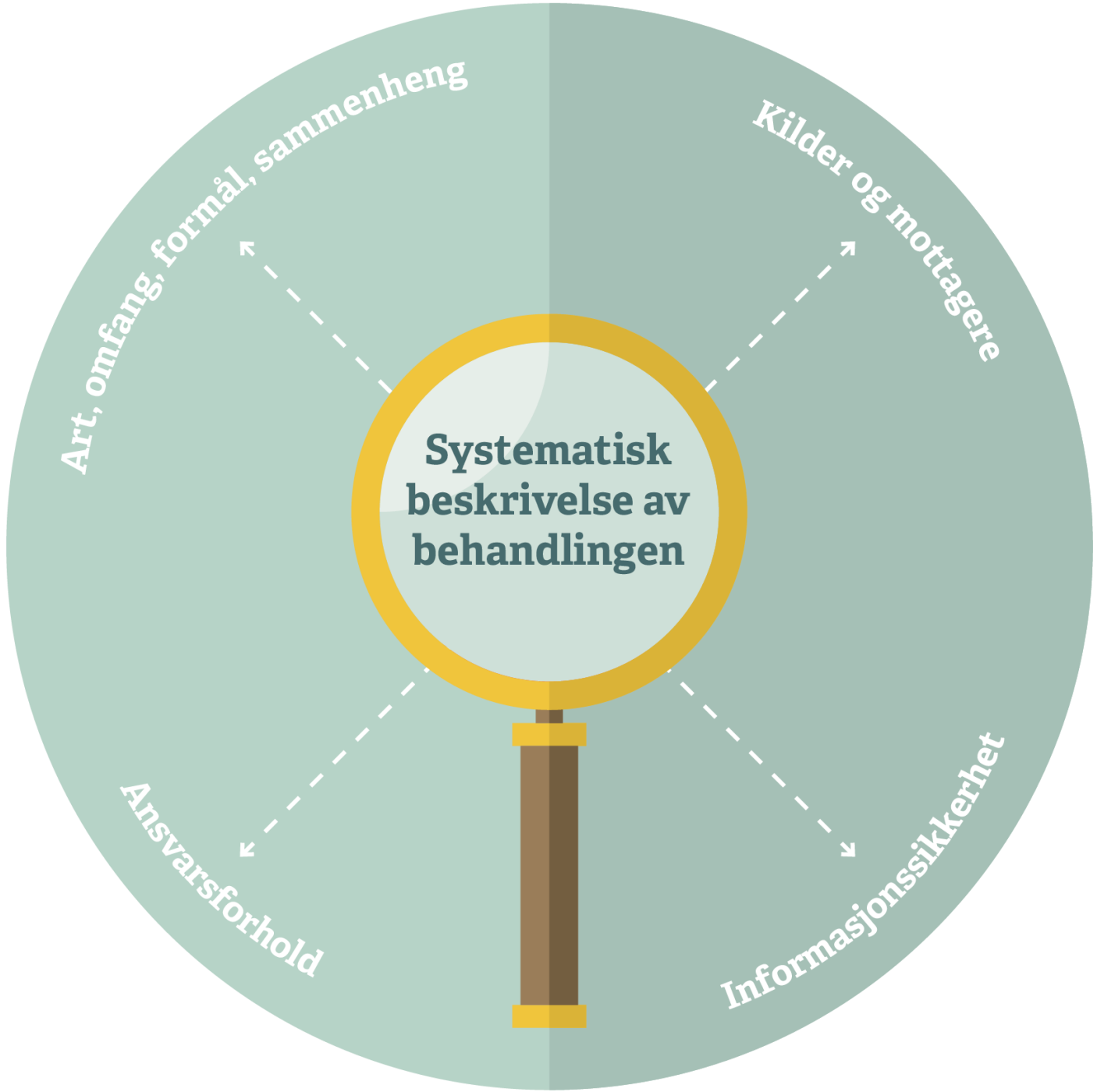
- Vurdering av nødvendighet og proporsjonalitet ved behandlingen:
- Lovlighet, rimelighet og åpenhet
- Formål og dataminimering
- Kvalitet og lagringsbegrensning
- De registrertes rettigheter
- De registrertes friheter

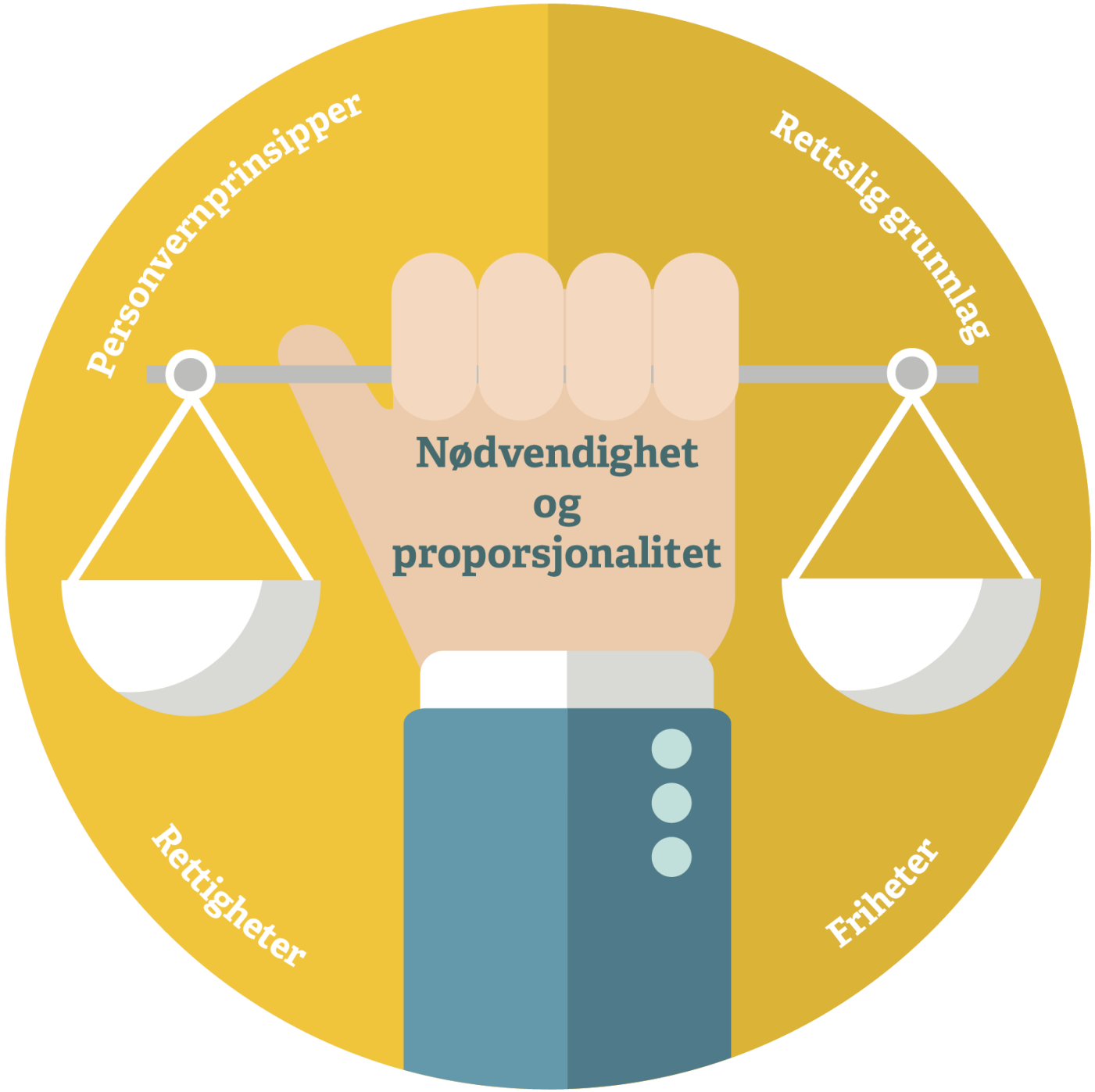


Vurdering av risiko for de registrertes rettigheter og friheter ut fra de registrertes perspektiv

De planlagte tiltakene for å håndtere risikoene

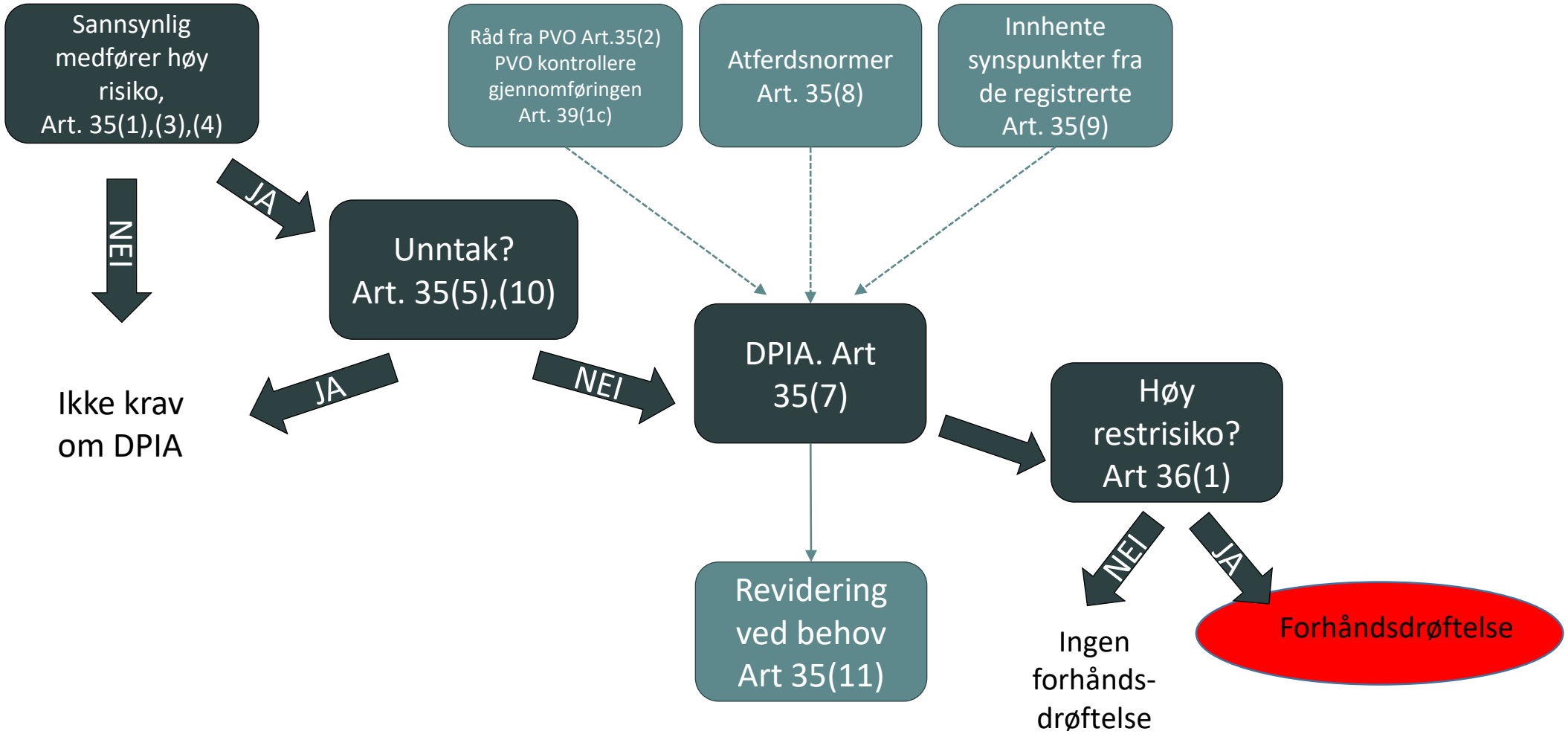
- Sammenstille og presentere funn
- Dokumentere hensynet til interessenter
- Ledelsens gjennomgang, beslutning og godkjenning


Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Ansvarsforhold
Informasjonssikkerhet


Personvernprinsipper
Rettslig grunnlag
Nødvendighet
og
proporsjonalitet
Rettigheter
Friheter


Åpenhet
Forutsigbarhet
Risiko for de registrertes rettigheter og friheter
Medbestemmelse
Tillit

Prosessen for DPIA



Camilla Nervik
22396929

cgn@datatilsynet.no

Følg oss:
datatilsynet.no
personvernbloggen.no
Twitter.com/datatilsynet