Grunnleggende kurs om GDPR og vern av personopplysninger

Advokat Hildegunn Y. Nygård
Tlf. 92440512 / epost: hyn@nho.no

6. November 2024

Personvernforordningen / GDPR

(GDPR – General Data Protection Regulation)

[2]

Personopplysningsloven § 2

Lovens saklige virkeområde

Loven gjelder for

- Helt eller delvis automatisert behandling av personopplysninger
- Annen behandling av personopplysninger når disse inngår eller skal inngå i et register
- Loven gjelder ikke
  - når en privatperson behandler personopplysninger til privat formål
  - for saker som behandles etter rettspleielovene (domstolene)

Alminnelige personopplysninger

SÆRLIGE KATEGORIER/SENSITIVE PERSONOPPLYSNINGER:

- rasemessig eller etnisk opprinnelse,
- politisk , filosofisk eller religiøs oppfatning
- helseforhold
- seksuelle legning eller orientering
- medlemskap i fagforening
- genetriske eller biometriske opplysninger for identifisering av person.

Den registrerte er:

> den personen som en opplysning eller vurdering kan knyttes til

GDPR Art. 4 nr. 2

NHO

> Behandling av personopplysning er enhver bruk av personopplysningen

- Innsamling/innhenting
- Registrering
- Lagring
- Analyse
- Sammenstilling med annen informasjon

Profilering

- Beslutningsgrunnlag
- Utlevering
- Sletting
- Osv…

GDPR Art. 83

Strenge reaksjoner ved overtredelser

- Inntil 20 M Euro / 4 % av årlig omsetning
- Pålegg om endringer

- **Sånn kan det gå:**
  Sjekkeappen Grindr må betale 65 000 000
- Sjekkeappen Grindr ble ilagt et overtredelsesgebyr på 65 millioner kroner av Datatilsynet for å ha levert ut personopplysninger om brukerne.

Hvem er behandlingsansvarlig?
Art. 4 nr. 7

> Den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes

Hvem er databehandler?

Art 4 nr 8

> Den som behandler personopplysningene på vegne av den behandlingsansvarlige

Personvernprinsippene

- **Lovlighet:** rettslig grunnlag
- **Rettferdighet**: forholdsmessighet mellom inngrepet og formålet
- **Åpenhet**: informasjonsplikter og innsynsrettigheter
- **Formålsbegrensning**: spesifikke, uttrykkelige angitte og berettigede, forbud mot uforenlige formål
- **Data minimering**: opplysningene skal være adekvate, relevante og nødvendige for formålet
- **Riktighet**: opplysningene skal være korrekte og oppdaterte
- **Lagringsbegrensning**: opplysningene skal anonymiseres eller slettes når behandlingen ikke er nødvendig for å nå formålet (unntak: arkiv og forskningsformål)
- **Integritet og fortrolighet**: tilstrekkelig sikkerhet mot uautorisert eller ulovlig behandling og utilsiktet tap, ødeleggelse eller skade
- **Ansvarlighet**: den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene overholdes

Behandlingsgrunnlag (rettslig grunnlag)

- Utgangspunktet: det er forbudt å behandle personopplysninger

- For å behandle personopplysninger, må man ha et lovlig grunnlag/rettslig grunnlag

Behandlingens lovlighet

a)**Samtykke**

b)For oppfyllelse av **avtale** den registrerte er part i, eller gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse

c)For oppfyllelse av **rettslig forpliktelse** som påhviler behandlingsansvarlig

d)For å verne den registrertes eller annen fysisk persons vitale interesser

e)Når nødvendig for å utføre oppgaver i allmennhetens interesse eller utøve offentlig myndighet

f)Interesseavveining – om behandlingsansvarlige formål har **berettig interesse** vs registrertes interesser

Samtykke som behandlingsgrunnlag

«Enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende»

Berettiget interesse som behandlingsgrunnlag

Bedriftens interesse

- berettiget?
- nødvendig?

Den registrertes interesse

- vil den bli negativt overrasket?
- hvor mange opplysninger?
- er det vurderinger?

Hjelpespørsmål – ja-siden

Har den registrerte bedt om at behandlingen finner sted?
Regner den registrerte med at behandlingen finner sted?
Vil den registrerte ha fordeler av behandlingen, som bedre varer eller tjenester?
Er behandlingen i den registrertes interesse?
Har bedriften og den registrerte samme interesse?
Er det noen tilknytning mellom bedriften og den registrerte (eller den registrertes arbeidsgiver) (for eksempel nåværende, tidligere eller potensiell kunde eller leverandør, ansatt eller konsulent)?
Gjelder behandlingen personen i egenskap av ansatt hos en kunde eller leverandør?
Er det et gjensidig forhold mellom bedriften og den registrerte?
Er det få opplysninger om den registrerte som vil bli behandlet?
Er det snakk om faktiske opplysninger?
Har den registrerte gitt opplysningene selv?
Er bedriften komfortabel med å gi god informasjon til den registrerte om behandlingen?
Gir bedriften god informasjon til den registrerte om behandlingen?
Er det enkelt for den registrerte å kontakte bedriften for å kontrollere behandlingen?

Hjelpespørsmål – nei-siden

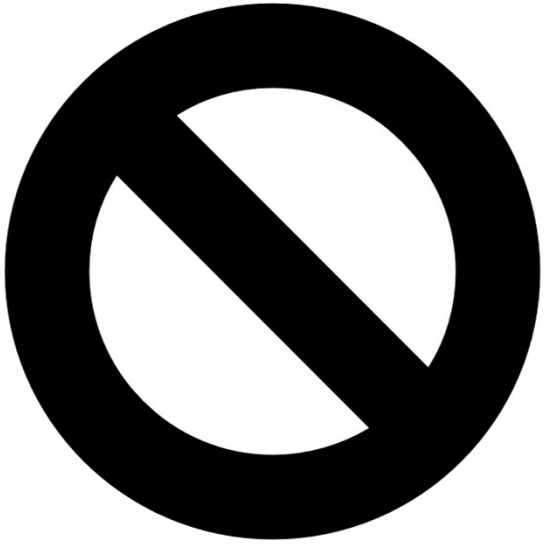
- Vil den registrerte bli overrasket over behandlingen?
- Vil den registrerte oppfatte behandlingen som negativ?
- Kan den registrerte oppfatte behandlingen som irriterende eller upassende – basert på forholdet mellom bedriften og den registrerte?
- Vil den registrerte oppfatte opplysningene som typisk private eller av følsom karakter?
- Inneholder opplysningene vurderinger av den registrerte?
- Vil det blir behandlet mange opplysninger om den registrerte?
- Er det snakk om en behandling som er uvanlig?
- Er det mulig for bedriften med en mindre inngripende behandling av opplysningene?

15

Særlige kategorier personopplysninger

BEHANDLING ER FORBUDT!

- **Men er likevel lov når:**
- Uttrykkelig samtykke
- Oppfylle forpliktelser innen arbeidsrett, trygderett, sosialrett
- Ivareta rettslig posisjon
- Ivareta viktige samfunnsinteresser



Overføring av personopplysninger utenfor EØS

- Overføring?
  - Behandlingsansvarlig/databehandler er underlagt GDPR
  - Tilgjengeliggjør eller sender personopplysningene til en annen behandlingsansvarlig/felles behandlingsansvarlig/databehandler
  - Dataimportøren er i et land utenfor EØS eller er en internasjonal organisasjon

- Sjekk liste over stater/områder med tilstrekkelig beskyttelsesnivå (Datatilsynet.no)
- Hvis ikke; må ha særskilt overføringsgrunnlag

Stater og områder med tilstrekkelig beskyttelsesnivå

Stater:

Andorra

Argentina

Guernsey

Isle of Man

Israel

Jersey

New Zealand

Sveits

Storbritannia

Uruguay

Områder / sektorer:

Canada	- hvis selskapet er underlagt PIPEDA, en kanadisk føderal lov for privat sektor
Færøyene	- hvis selskapet er underlagt den færøyske loven om behandling av personopplysninger
Japan	- hvis selskapet er underlagt APPI, en japansk lov for privat sektor
Sør-Korea	- hvis selskapet er underlagt den sørkoreanske loven om behandling av personopplysninger
USA	– hvis mottaker står på listen over virksomheter som er sertifisert under EU-U.S. Data Privacy Framework

Hva er særskilt overføringsgrunnlag?

1. Standard personvernbestemmelser vedtatt av EU-kommisjonen
2. Bindende virksomhetsregler
3. Godkjente adferdsnormer
4. Godkjent sertifiseringsmekanisme sammen med bindende og håndhevbar avtale
5. Avtalevilkår godkjent av Datatilsynet og Personvernrådets tilslutning

Schrems II – dommen:

- Vil overføringsgrunnlaget sikre personvernet i praksis eller begrenser for eksempel lovbestemmelser i mottakerlandet personvernet?
  - Tekniske tiltak
    - Kryptering
    - pseudonymisering
  - Juridiske tiltak
    - Avtalevilkår om nøkkelhåndtering
    - Avtalt forbud mot re-identifisering ved pseudonymisering
  - Organisatoriske tiltak
    - Interne rutiner og internkontroll
    - Rutiner ved utleveringsbegjæringer

Behandlingsformål

- Personopplysninger skal samles inn for
  - spesifikke,
  - uttrykkelig angitte og
  - berettigede formål
- og ikke viderebehandles på en måte som er uforenlig med disse formålene
    - Uten samtykke eller lovhjemmel

•Momenter for vurdering av om nytt formål er uforenlig med det opprinnelige:

•Er det forbindelse mellom opprinnelig og nytt formål?

•i hvilken sammenheng er opplysningene samlet inn?

•personopplysningenes art, behandles det for eksempel *sensitive personopplysninger?*

•mulige konsekvenser av den tiltenkte viderebehandlingen?

•blir opplysningene beskyttet ved hjelp av f.eks. *kryptering* eller *pseudonymisering?*

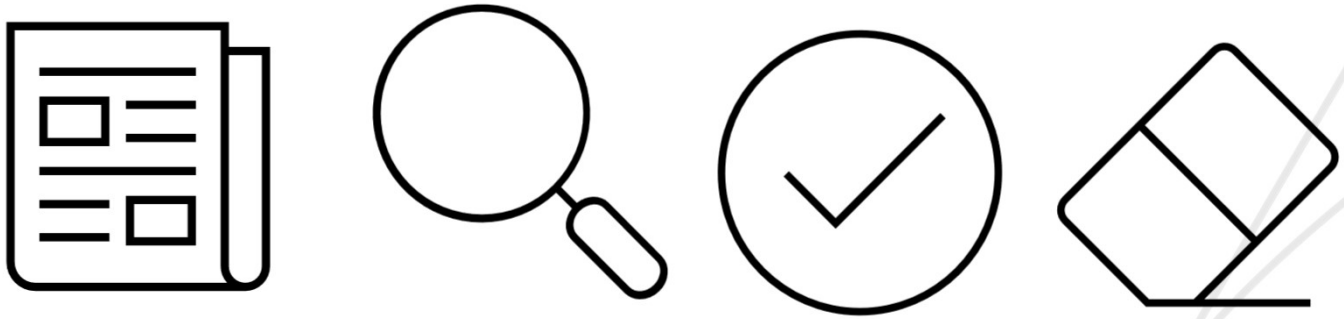
Rt-2013-143 Avfallsservice

- GPS/elektronisk logg i renovasjonsbilene
- Formålet med GPS: rapportere håndtering av søppeldunker
- GPS/elektronisk logg ble brukt til å avdekke avvik i arbeidstaker sine timelister, og arbeidstaker ble oppsagt
- Høyesterett: bruk av personopplysninger fra GPS i sammenstilling med timelister for å kontrollere arbeidstiden var i strid med formålet med GPS-loggingen, og ulovlig

PVN-2017-18 Nobina Norge

- GPS med individuelt sjåførkort i bussene
  - Rute, bil/sjåfør, kundetransaksjoner og tidspunkt på holdeplasser
- GPS ble brukt til å avdekke avvik i arbeidstaker sine timelister
- Kontrolltiltak drøftet med tillitsvalgte og informert de ansatte
  - Formål: forebygge og avdekke avvik fra interne regler og rutiner, avklare driftsavvik, driftsbrudd og eksterne anslag
- Bruk av opplysningene i GPS lå derfor innenfor de ansattes rimelige forventninger om hva opplysningene kunne brukes til

Den registrertes rettigheter



Informasjon Innsyn Retting Sletting

Personvernerklæringen – informasjon til de registrerte om behandlingen

- Foretaksnavn og kontaktopplysninger
- Formål med behandlingen
- Behandlingsgrunnlag for behandlingen
- Eventuell mottaker av opplysninger?
- Utlevering til land utenfor EØS?
- Oppbevaringsperiode for opplysningene
- Eventuelle automatiserte individuelle avgjørelser/profilering

De registrertes rettigheter til å

- be om tilgang til opplysningene som er lagret om dem
- be om retting av opplysninger som er uriktige
- be om sletting av opplysninger
- be om begrensning av behandling
- protestere mot at opplysninger blir behandlet
- be om utlevering av opplysninger til seg selv eller til andre
- trekke tilbake eventuelle samtykker til behandling
- klage til Datatilsynet i Norge (eller tilsvarende organ der den registrerte bor eller der regelbrudd har funnet sted) på behandling av personopplysninger

GDPR Art 15

Innsynsrett

- Den registrerte har rett til å få vite hvilke personopplysninger som behandles

  - De personopplysningene som behandles
  - Formålene med behandlingen
  - Hvem opplysningene har eller vil bli utlevert til
  - Kategorier av personopplysninger
  - Hvor lenge opplysningene vil bli lagret
  - Hvor opplysningene kommer fra
  - Ev. automatiserte avgjørelser /profilering

Personopplysningsloven § 16 bokstav f

Unntak for interne dokumenter:

- «utelukkende finnes i tekst som er utarbeidet for

  - intern saksforberedelse, og som heller
  - ikke er utlevert til andre,
  - så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser»

GDPR Art 16 og 19

Retting

- Uriktige personopplysninger skal
  - Rettes
  - Kompletteres

- Plikt til å varsle mottakere når retting er utført
  - Med mindre umulig eller uforholdsmessig

GDPR Art. 17

Sletting av personopplysninger

- Opplysninger kan bare oppbevares så lenge som man trenger de for å oppnå formålet med opplysningene.
- Opplysningene må slettes dersom et samtykke trekkes
- Den registrerte kan dessuten kreve opplysninger slettet dersom det ikke finnes mer tungtveiende berettigede grunner til å beholde de

    - interesseavveining

PVN-2018-15

- Lærer ved videregående skole som krevde opplysninger om seg i personalmappen slettet etter at han var sluttet ved skolen
- Opprinnelig formål med å ha opplysninger i personalmappen: personaloppfølging
- Formål med fortsatt lagring etter avslutning:
  - skolens behov for å dokumentere saksbehandlingshistorikk i saken ved senere klage eller søksmål
  - Behov for å ha opplysningene hvis læreren senere søker om ansettelse igjen hos samme arbeidsgiver?

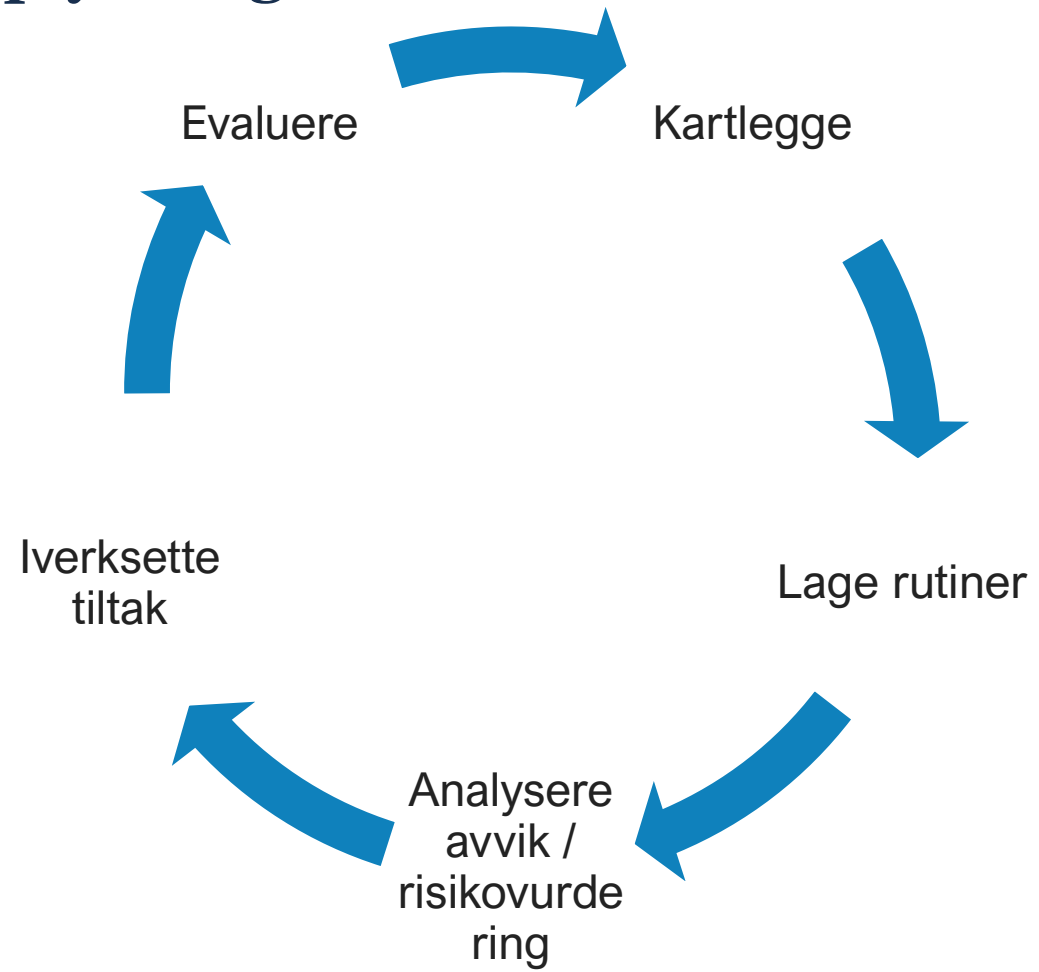
GDPR Art. 12

Hvordan ivareta disse rettighetene?

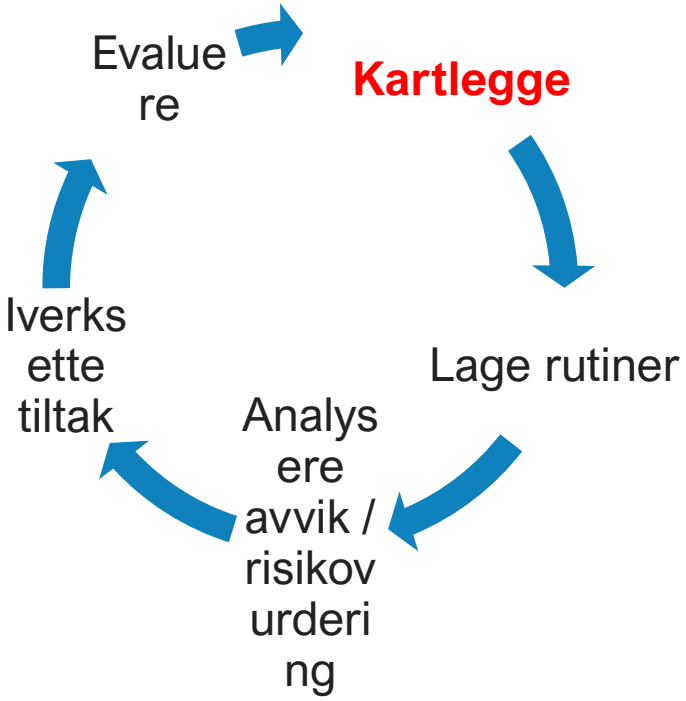
- Svar uten ugrunnet opphold og senest en måned etter mottak av henvendelsen
- Rett mottaker?
- Gratis
- Lett tilgjengelig og forståelig informasjon
- Rett til informasjon om/innsyn i opplysninger – ikke dokumenter

Ivaretakelse av personopplysningene dere behandler

Det skal
være tilfredsstillende
teknisk og
organisatoriske
tiltak for å sikre og
påvise at
behandlingen utføres
i samsvar med
personvernreglene



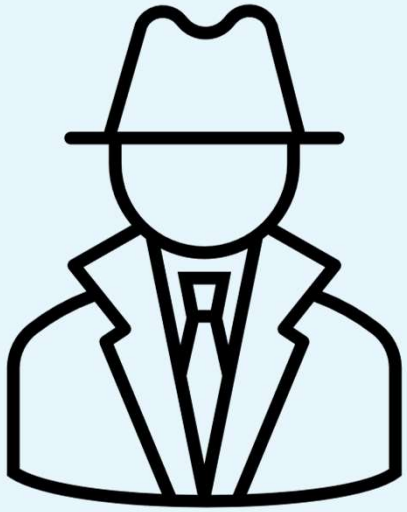
Krav til protokoll over behandlingsaktiviteter



- For virksomheter med 250 ansatte eller mer
- Gjelder også virksomhet med færre enn 250 ansatte dersom;
  - behandlingen trolig vil medføre en risiko for «de registrertes rettigheter og friheter»
  - Behandlingen ikke bare skjer leilighetsvis
  - Behandlingen omfatter sensitive personopplysninger
  - Behandlingen omfatter opplysninger om straffedommer og lovovertredelser

NHO

Hvem må ha personvernombud?



- Offentlig virksomhet
- Selskaper hvor kjerneaktiviteten involverer
  - Storskala behandling av sensitive personopplysninger
    - Sykehus
  - Storskala (jevnlig og systematisk) monitorering/profilering av individer
    - Kameraovervåking
    - Profilering i forbindelse med kredittvurdering
    - Sporing av lokasjon i mobilapplikasjoner

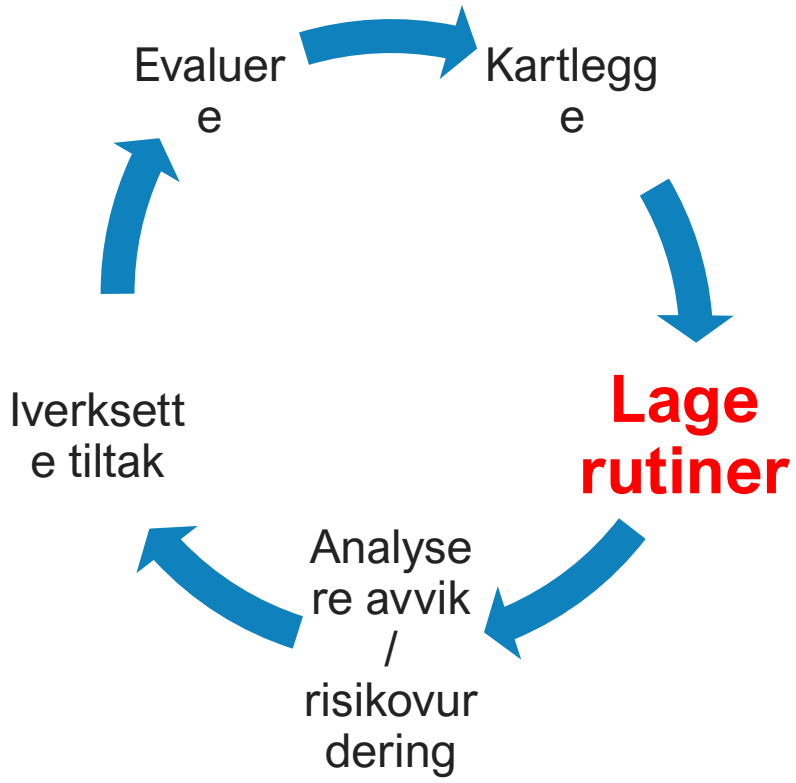
NHO

Vurdering av personvernkonsekvenser:
«høy risiko for de registrertes rettigheter og friheter»

- Krav om vurdering ved (bl.a.):
    - Systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
    - Behandling av sensitive personopplysninger i stort omfang
    - Systematisk overvåking av offentlig område i stort omfang

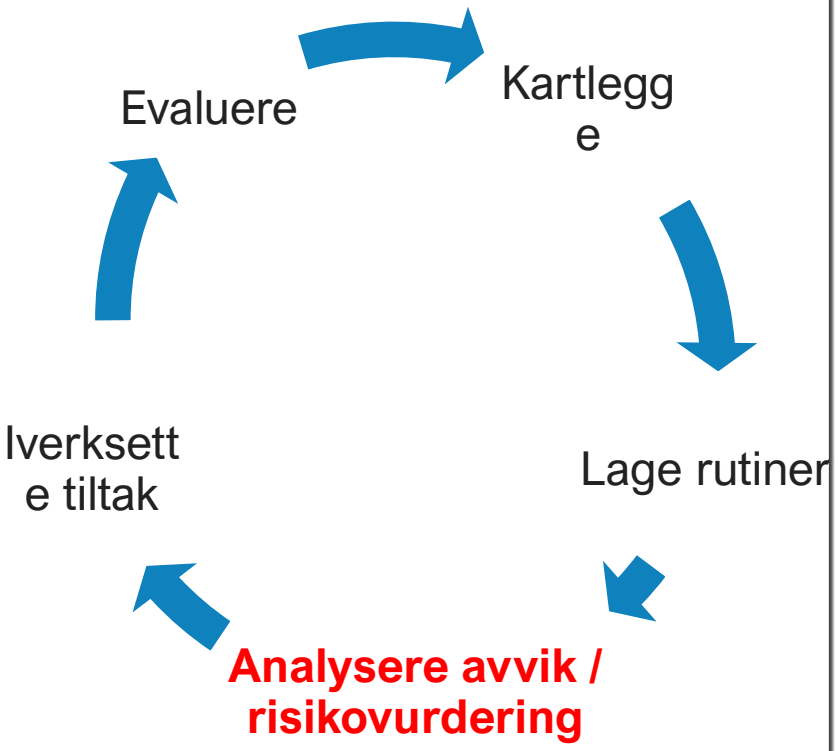
1. Evaluering eller poengsetting
2. Automatiske beslutninger
3. Systematisk monitorering
4. Særlige kategorier eller svært personlige personopplysninger
5. Personopplysninger i stor skala
6. Matching/sammenstilling av datasett
7. Sårbare registrerte
8. Innovativ bruk / anvendelse av ny teknologisk eller organisatorisk løsning
9. Behandlingen hindrer rettighet/tjeneste

Retningslinjer for vern av personopplysninger



- Beskrivelse av rutiner for å ivareta personvernet, herunder:
  - Hvem er ansvarlig for behandlingen og hvem tar imot krav fra registrerte?
  - Hvilke behandlingsgrunnlag og formål har vi?
  - Hvilke slette-rutiner har vi?
  - Hva er rutinene våre for utlevering, innsyn og retting av personopplysninger?
  - Hva er våre rutiner for å ivareta informasjonssikkerheten?
  - Rutine for innsyn i ansattes e-post.
  - Osv.

Risikovurdering

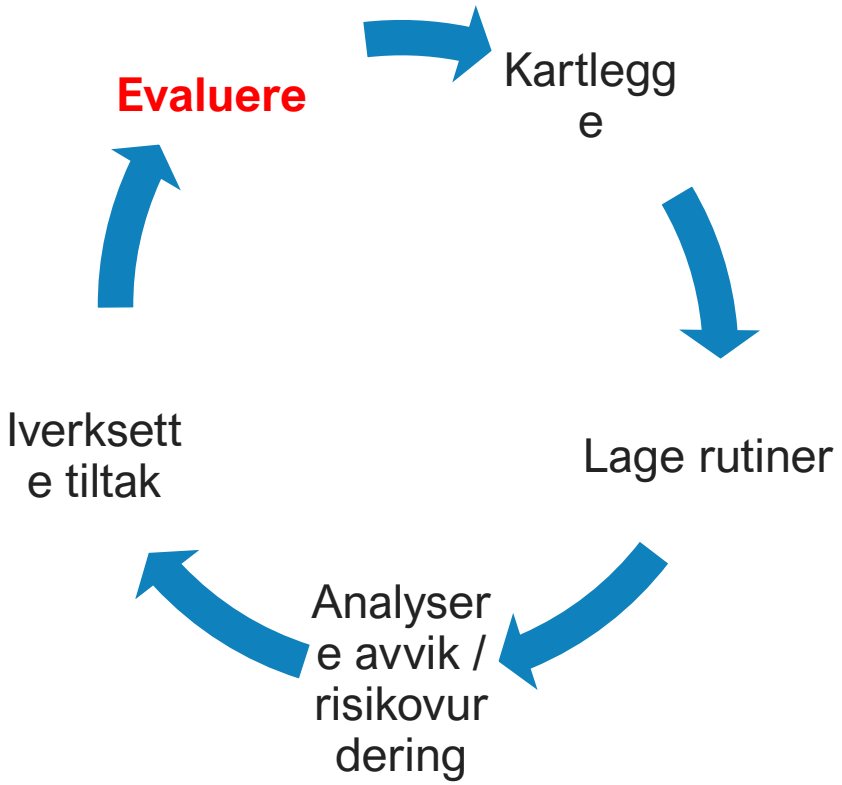


Sannsynlighet	Konsekvens			
	1. Ufarlig	2. Uheldig	3. Alvorlig	4. Kritisk
1. Lite sannsynlig				
2. Mindre sannsynlig				
3. Sannsynlig				
4. Svært sannsynlig				

Ivareta tilstrekkelig sikkerhetsnivå

- Virksomheten skal gjennomføre passende **tekniske** og **organisatoriske** tiltak for å oppnå et sikkerhetsnivå som svarer til risikoen knyttet til virksomhetens behandling av personopplysninger.
- Informasjonssikkerheten skal ivareta
  - Konfidensialitet
  - Skjerming for uvedkommende
  - Integritet
  - At opplysningene ikke endres utilsiktet/av uvedkommende
  - tilgjengelighet

Evaluering og vurdering av informasjonssikkerheten



- Kontinuerlig prosess:
  - Oppdatering og evaluering
  - Endret/opphørt behandling?
  - Erfaringer siden sist?
  - Endring av regelverk?
  - Ny teknologi/nytt trusselbilde?
  - Annet – forbedringsområder dere oppdager?

GDPR Art 4 bokstav l

Brudd på personopplysningssikkerheten - hva er det?

- *utilsiktet eller ulovlig*

  tilintetgjøring,
  tap,
  endring,
  ulovlig spredning av eller tilgang til

  personopplysninger

GDPR Art 33 og 34

Brudd på personopplysningssikkerheten - hva nå?

- Avviksmelding til Datatilsynet innen 72 timer
  - «**med mindre det er lite trolig** at bruddet vil medføre en **risiko** for fysiske personers rettigheter og friheter»
- Avviksmelding til den registrerte uten ugrunnet opphold
  - «Dersom det er **sannsynlig** at bruddet på personopplysningsforskriften vil medføre **høy risiko** for fysiske personers rettigheter og friheter»

Nyttige linker:

- www.arbinn.no
- www.lovdata.no
- www.nho.no

NHOs regionkontor

- www.nho.no/vestlandet
- www.nho.no/innlandet
- www.nho.no/arktis
- www.nho.no/agder
- www.nho.no/rogaland
- www.nho.no/trondelag
- www.nho.no/nordland
- https://www.nho.no/regionkontor/nho-more-romsdal/
- https://www.nho.no/regionkontor/nho-vestfold-telemark/
- https://www.nho.no/regionkontor/nho-viken-oslo/

42