



Oslo

Et dypdykk i grunnleggende personvernprinsipper

Linda Mari Knutsen
Maryke Silalahi Nuth

FIN v/seksjon for Informasjonssikkerhet
og IKT (ISI)



Foto: Thomas Ekström

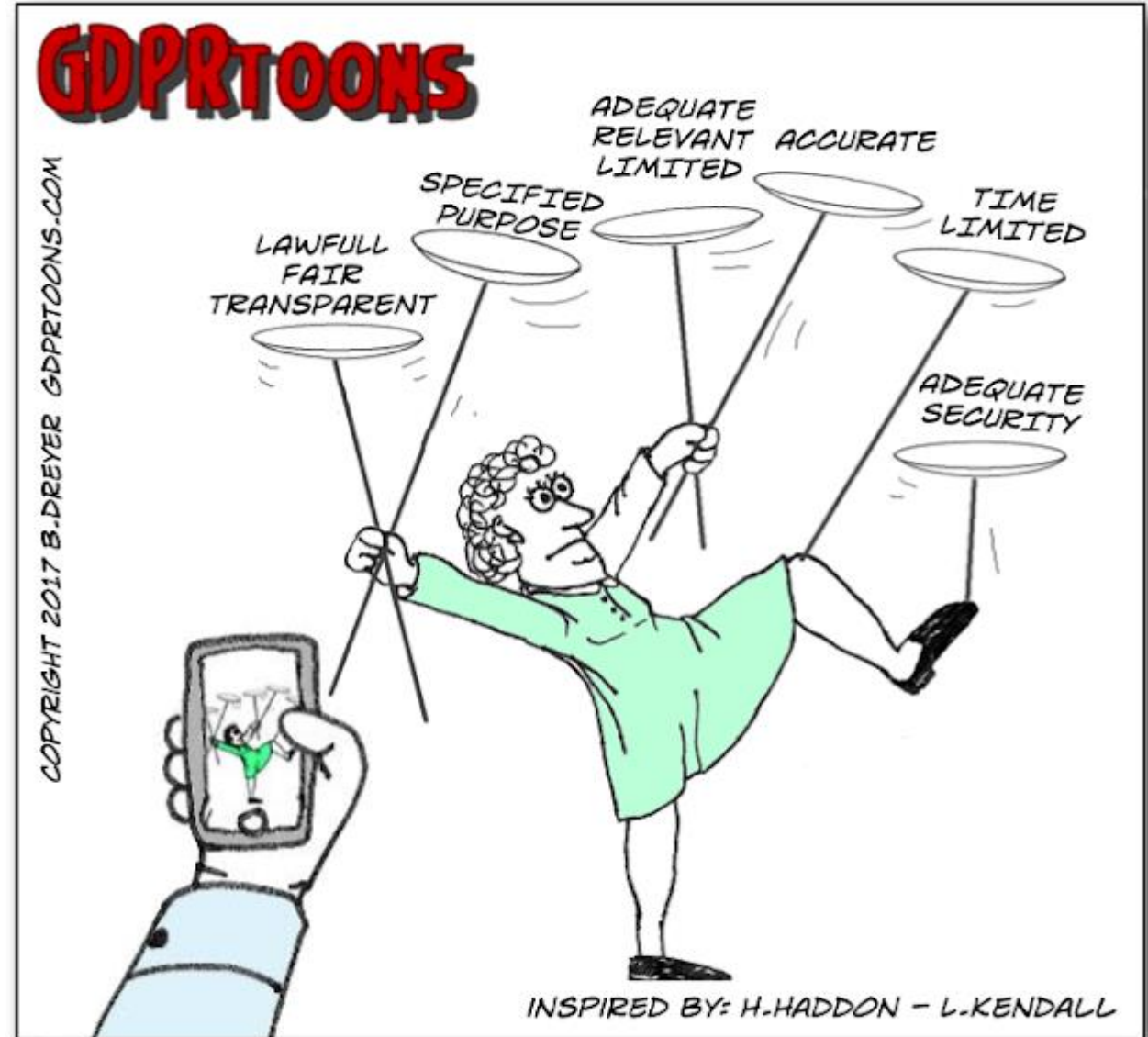
Før vi starter:

- Kort om Seksjon for informasjonssikkerhet og IKTs arbeid med personvern
- Spørsmål kan stilles i chatten, så besvarer vi dem underveis!
- Dere kan også sende oss spørsmål på e-post som besvares i etterkant av kurset



Agenda for kurset:

- ▶ Hvorfor har vi personvernprinsipper?
- ▶ Hvilke personvernprinsipper har vi?
- ▶ Nærmere om de 7 grunnleggende prinsippene



Hvorfor har vi personvernprinsipper?

- ▶ Alle reglene i personvernforordningen bygger på grunnleggende prinsipper for personopplysningsvern
 - Alle virksomheter som behandler personopplysninger må derfor opptre i samsvar med disse prinsippene
- ▶ Med GDPR ble prinsippene inntatt som egen bestemmelse i artikkel 5, men er de egentlig nye?
 - OECD guidelines fra 1980: flere av dagens prinsipper ble nedfelt. Disse var primært politiske og retningsgivende for nasjonal lovgivning.
 - Deretter Direktiv 95 (tidligere personopplysningsloven): del av felles direktiv, rettskildemessig betydning pga stor grad lagt til grunn i rettspraksis
 - Hva betyr det at prinsippene er inntatt som en egen bestemmelse?

Nærmere om de enkelte personvernprinsippene i personvernforordningen

De 7 grunnleggende personvernprinsipper



**Lovlighet, rettferdighet
og åpenhet**



Formålsbegrensing



Dataminimering



Riktighet



Lagringsbegrensing



**Konfidensialitet og
integritet**



Ansvarlighet



Lovlighet,
rettferdighet og
åpenhet

Prinsippet om **Lovlighet, rettferdighet og åpenhet**

- ▶ Den behandlingsansvarlige skal sørge for at personopplysninger behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte



**Lovlighet,
rettferdighet og
åpenhet**

Nærmere om prinsippet om Lovlighet

- ▶ Må finnes et rettslig grunnlag for behandlingen av personopplysninger
- ▶ Personvernforordningen art 6 regulerer de ulike tilfeller det skal anses som lovlig å behandle personopplysningene.
 - Minst ett må være oppfylt slik at behandlingen anses som lovlig
- ▶ Dersom særlige kategorier/sensitive personopplysninger behandles må også minst ett vilkår i art 9 være oppfylt.



Behandlingsgrunnlag etter artikkel 6



Samtykke

- frivillig
- spesifikt
- informert
- utvetydig



Hjemmel i lov/forskrift

- Rettslig plikt /offentlig myndighet
- Klarhetskrav



Avtale

- Den registrerte må være del av avtalen
- Nødvendig for å utføre den etterspurte tjenesten



Ivareta vitale interesser

- Svært snevert
- Liv og død/stor helsefare



Utøve oppgave i allmenhetens interesse/ offentlig myndighet

- Offentlig myndighet
- Noen tilfeller private virksomheter
- Lovlig



Berettiget interesse

- Lovlig
- Klart definert
- Minst inngripende mulighet
- Interesseavveining



**Lovlighet,
rettferdighet og
åpenhet**

Barns samtykke etter artikkel 8

- ▶ Der informasjonssamfunnstjenester er rettet mot barn og samtykke er behandlingsgrunnlaget, må samtykke innhentes fra foreldre eller foresatte dersom barna er under 13 år gamle.
- ▶ Informasjonssamfunnstjeneste: kommersiell tjeneste som leveres elektronisk, på avstand og etter individuell forespørsel. For eksempel sosiale medier.
- ▶ I slike tilfeller må virksomheten iverksette rimelige tiltak for å verifisere at samtykke er gitt fra rette vedkommende.



**Lovlighet,
rettferdighet og
åpenhet**

Kort om personvernforordningens art 9

- ▶ I utgangspunktet forbudt å behandle særlige kategorier av personopplysninger, også kalt sensitive personopplysninger
- ▶ Men er flere unntak fra forbudet i art 9 nr. 2
 - Poenget: må foreligge et særskilt grunnlag i tillegg til behandlingsgrunnlag for å behandle disse typer personopplysninger
- ▶ Merk: Hvis forordningen sier at behandlingen krever hjemmel i lov, stilles det også visse krav til loven eller lovens innhold
 - Det betyr at en hvilken som helst lovhjemmel er ikke nødvendigvis tilstrekkelig.

Artikkel 9 – eksempler på behandlingsgrunnlag



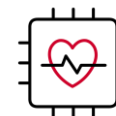
Lovlighet,
rettferdighet og
åpenhet



**Uttrykkelig
samtykke fra den
registrerte**



**Oppfylle og utøve
sine
arbeidsrettslige,
trygderettslige og
sosialrettslige
plikter og
rettigheter**



**Nødvendig i
forbindelse med...
ytelse av helse-
eller
sosialtjenester**



**Lovlighet,
rettferdighet og
åpenhet**

Hvordan kan virksomheten oppnå prinsippet om Lovlighet?

- ▶ Virksomheten må iverksette tiltak som kan ivareta kravet om at behandlingen ikke går videre enn hva behandlingsgrunnlaget gir adgang til
- ▶ For eksempel:
 - Organisatorisk tiltak i form av rutiner som sørger for at virksomheten vurderer behandlingsgrunnlaget før behandlingen starter.
 - Ved bruk av Samtykke kan virksomheter etablere tiltak som kontrollerer hva Samtykke gir adgang til, samt tekniske sperrer for behandlinger som går ut over samtykkets innhold.

Spørsmål til deltakerne:



**Lovlighet,
rettferdighet og
åpenhet**

Vurderer din virksomhet hvilket
behandlingsgrunnlag som er gjenstand for
behandlingen av personopplysninger?





Lovlighet,
rettferdighet og
åpenhet

Eksempel på hvordan virksomheten kan oppfylle prinsippet om Lovlighet

▶ Saksbehandlingssystem:

- Ved behandling av ansattopplysninger vil berettiget interesse og arbeidsgivers styringsrett være behandlingsgrunnlaget
- Utførelse av oppgaver i saksbehandlingssystemet vil i stor grad lovhjemmel for relevant saksområde være aktuell som behandlingsgrunnlag

▶ Arrangementer:

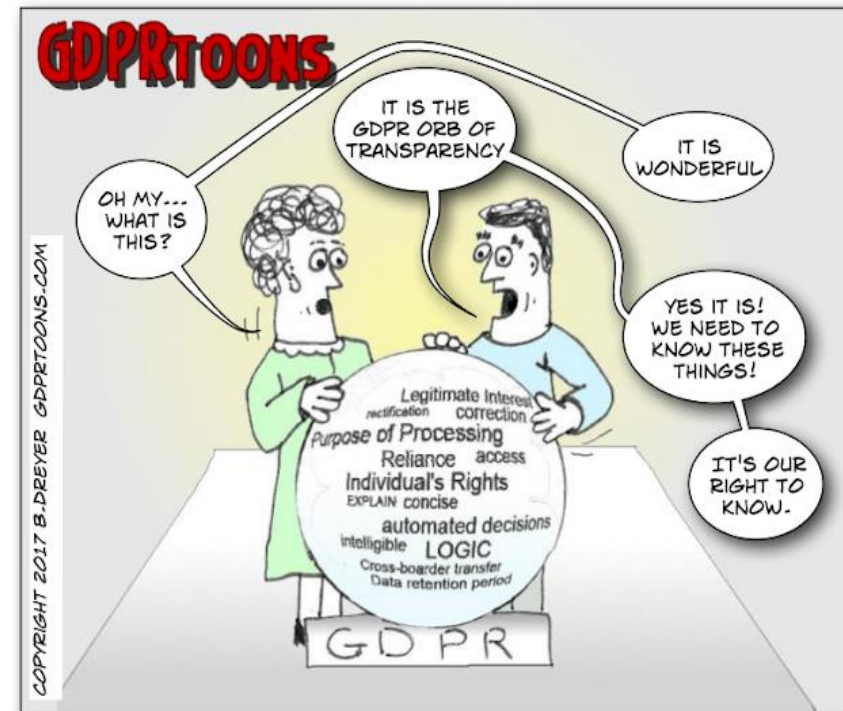
- Ved behandling av ansattopplysninger vil hjemmelsgrunnlag kunne være ansattes arbeidsavtale knyttet til utøvelse av sitt arbeid
- Ved behandling av personopplysninger om deltakere vil samtykke sannsynligvis være det rette behandlingsgrunnlaget.
 - For eksterne foredragsholdere vil det også kunne være oppdragsavtale som er behandlingsgrunnlaget



Lovlighet,
rettferdighet og
åpenhet

Rettferdighet og åpenhet

- ▶ Behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og rimelige forventninger.
- ▶ Behandlingen skal også være gjennomiktig (transparent) og forståelig for de registrerte,
 - Det betyr: den skal ikke foregå på skjult eller manipulerende måte.
- ▶ Må sees i sammenheng med kap 3 i personvernforordningen om de registrertes rettigheter.





Lovlighet,
rettferdighet og
åpenhet

Hvordan kan virksomheten oppnå prinsippene Rettferdighet og Åpenhet?

- ▶ Virksomhetene kan iverksette tiltak som ivaretar rettigheter for de registrerte (innbygger, ansatte etc) etter personvernregelverket, eller tiltak som ivaretar grunnleggende menneskerettigheter (friheter).
 - Funksjonalitet for å tilegne seg informasjon på nettsider
 - Personvernerklæring
 - Tilrettelegge for innsynsforespørsler
- ▶ For å sikre åpenhet kan bør virksomhetene være åpne om hvilke personopplysninger som behandles og dersom man bruker spesielle verktøy/metoder for å oppnå formålet med behandlingen (eks. profilering)

Spørsmål til deltakerne:



**Lovlighet,
rettferdighet og
åpenhet**

Hvordan gir din virksomhet informasjon til
de registrerte når det behandles
personopplysninger?





Lovlighet,
rettferdighet og
åpenhet

Eksempel på hvordan virksomheten kan oppfylle prinsippet om Rettferdighet og Åpenhet

▶ Saksbehandlingssystem:

- Arbeidsgiver kan gi informasjon til ansatte på intranettsiden om hvilke behandlinger som forekommer, type opplysninger, lagringstid etc.
- Virksomhetens personvernerklæring – informasjon til den registrerte som viser behandling etc.
 - Særlig dersom man benytter delvis automatisert behandling

▶ Arrangementer:

- Informasjon til de registrerte (deltakerne)
 - Informasjon må være uavhengig av samtykkeerklæring



Prinsippet om **Formålsbegrensning**

- ▶ Personopplysninger skal kun behandles for spesifikke, uttrykkelig angitte og berettigede (legitime) formål
- ▶ Virksomheten må identifisere og beskrive så presist så mulig ethvert formål med behandling av personopplysninger
 - Forklart slik at man oppnår entydig forståelse av hva opplysningene skal benyttes til
 - Ha et rettslig grunnlag, i samsvar med etiske og rettslige samfunnsnormer

Gjenbruk av personopplysninger (deling av data)



Formålsbegrensning

- ▶ Utgangspunktet: Må være «forenelig med opprinnelig formål»
- ▶ Dersom «uforenelig» må det være adgang til viderebehandling i lov eller det må innhentes nytt samtykke fra den registrerte.
- ▶ ikke tilstrekkelig med et alminnelig behandlingsgrunnlag og et eventuelt supplerende rettslig grunnlag i den forbindelse; det **kreves i tillegg et grunnlag** for viderebehandlingen





Sentrale momenter i vurderingen om behandlingen er «uforenelig» (art 6 nr 4)

- ▶ Om det er forbindelse mellom opprinnelig og nytt formål
- ▶ I hvilken sammenheng opplysningene er samlet inn
- ▶ Personopplysningenes art, for eksempel om det behandles sensitive personopplysninger
- ▶ Mulige konsekvenser av den tiltenkte viderebehandlingen
- ▶ Om opplysningene blir beskyttet ved hjelp av for eksempel kryptering eller pseudonymisering





Formålsbegrensning

Behandling av personopplysninger til arkiv- og statistikkformål

- ▶ Gjenbruk av personopplysninger til arkivformål i allmenhetens interesse, vitenskapelige eller historiske forskningsformål eller til statistiske formål er ikke uforenelig med opprinnelig formål dersom behandlingen er underlagt nødvendige garantier.
- ▶ Arkivformål kommer i tillegg til opprinnelig formål med behandlingen
- ▶ Statistiske formål: enkelte ganger lovpålagt, for eksempel rapporteringsplikt



Tiltak virksamheten kan iverksette for å ivareta prinsippet om Formålsbegrensning

- ▶ Tiltak som gjør at det eksplisitt blir tatt stilling til hva slags prosessering av personopplysninger som er innenfor de angitte formål, og hva som ikke er det.
 - Tekniske tiltak kan være å etablere sperrer mot behandling som ikke er innenfor formålet, for eksempel utlevering av personopplysninger
- ▶ Tiltak som sikrer at det som standard kun behandles opplysninger til det som er forutsatt fra starten.

Spørsmål til deltakerne:



Formålsbegrensing

Når din virksomhet behandler personopplysninger har dere utfordringer med å tydeliggjøre formålet/ene med behandlingen?





Eksempel på hvordan ivareta prinsippet om Formålsbegrensning

► Saksbehandlingssystem:

- Behandling av personopplysninger kan ha flere formål
- Behandling av ansattopplysninger kan formålet være å autentisere den ansatte
- Behandling av personopplysninger knyttet til den enkelte oppgave/sak vil formålet/-ene ofte være regulert i regelverket.
- Videre kan det være formål som lovpålagt rapporteringsplikt, uttrekk av statistikk, kvalitetsforbedring mv.

► Arrangement:

- Formålet må være spesifikt tilknyttet arrangementet
- Kan også være andre formål ut over selve arrangement, for eksempel servering av lunsj
- Også formål å behandle personopplysninger i etterkant av arrangementet:
 - Benytter data til for eksempel statistikk, oppfølging av deltakere, smittesporing

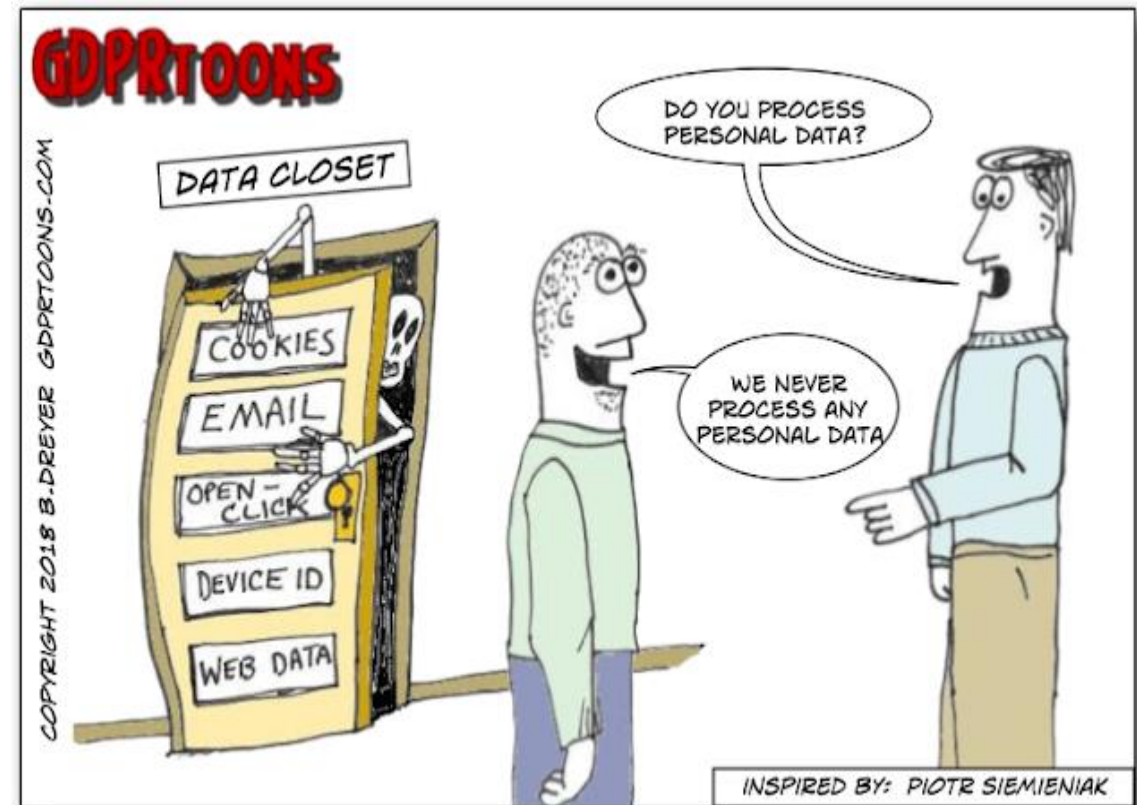
PAUSE 10 MINUTTER!





Prinsippet om **Dataminimering**

- ▶ Personopplysninger som innsamles er adekvate, relevante og begrenset til det som er nødvendig for formålet/-ne.
- ▶ Det betyr: hvis personopplysningene ikke er nødvendig å behandle for å oppnå formålet, skal virksomheten heller ikke behandle dem.
- ▶ Hensynet bak: å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.





Tiltak virksomheten kan iverksette for å ivareta prinsippet om Dataminimering

- ▶ Tekniske tiltak: funksjonalitet i løsninger som sikrer at det ikke innhentes personopplysninger om flere personer enn nødvendig, eller at funksjonaliteten stilles inn slik at kun relevante og nødvendige personopplysninger innhentes.
- ▶ Organisatoriske tiltak: etablere rutiner som gjør at ansatte tar stilling til at det kun samles inn relevante og nødvendige personopplysninger, eller om det i det hele tatt er nødvendig å behandle personopplysninger

Spørsmål?



Dataminimering

Hvordan oppnår din virksomhet
kravet til Dataminimering?





Eksempler på hvordan virksomheter kan ivareta prinsippet om Dataminimering

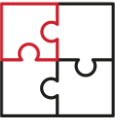
▶ Saksbehandling:

- Ansattopplysninger: virksomheten sørger for at kun relevante og nødvendige opplysninger behandles for å autentisere den ansatte. For eksempel vil man ikke ha behov for å benytte personlig informasjon om den ansatte, herunder familierelasjon, adresse etc
- Ved utførelse av oppgaver til virksomheten må de ansatte påse at kun relevant informasjon innhentes dersom de er i dialog med innbyggere
- Systemet bør også ha funksjonalitet som sørger for å innhente relevant og nødvendig informasjon der det er mulig, for eksempel ved søknadsskjema fra innbygger, utlevering av informasjon fra andre (nasjonale) registre mv.

▶ Arrangement:

- Virksomheten påser at det kun er de mest nødvendige opplysninger om deltakerne som samles inn ifbm arrangementet, for eksempel navn, tlfnr, virksomhetstilhørighet og virksomhetens adr. Det vil eksempelvis ikke være nødvendig med fødselsnummeret til deltakerne

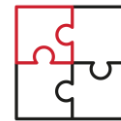
Prinsippet om **Riktighet**



Riktighet

- ▶ Personopplysninger skal være så korrekte og oppdaterte som nødvendig for å oppnå formålet med behandlingen .
- ▶ Det betyr: Dersom opplysninger er uriktige sett opp mot de formål de behandles for skal virksomheten straks slette eller rette disse opp.
- ▶ Merk: er opplysningene utlevert til andre må virksomheten sørge for at også disse får beskjed om retting eller sletting

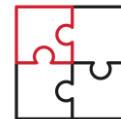
Tiltak virksomheten kan iverksette for å ivareta prinsippet om Riktighet



Riktighet

- ▶ Tekniske tiltak som kan iverksettes for å sørge for at personopplysningene er korrekte og oppdaterte er at virksomhetens løsning regelmessig varsler brukerne om å kontrollere sine personopplysninger. For eksempel ved innlogging via ID-porten.
- ▶ Andre tiltak kan være å tilrettelegge for å kunne slette eller korrigere opplysningene straks dersom personopplysningene er uriktige.

Spørsmål til deltakerne:

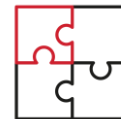


Riktighet

Hvordan sørger din virksomhet for at prinsippet om riktighet ivaretas ved behandling av personopplysninger?



Eksempler på hvordan ivareta prinsippet om Riktighet



Riktighet

▶ Saksbehandlingssystem:

- Ved bruk av ansattopplysninger kan virksomhetens HR-system benyttes.
- Saksbehandlingssystemet bør ha rutiner for å korrigere og slette personopplysninger som er feilaktige.
- For personopplysninger som behandles for å utføre oppgaver til virksomheten kan tekniske tiltak være avsjekk med Folkeregisteret.

▶ Arrangement:

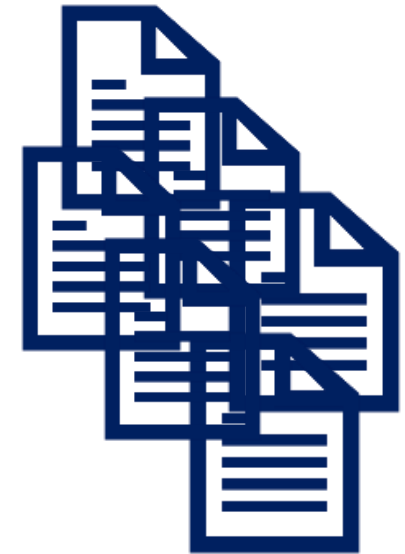
- Ansvarlig virksomhet kan be om oppdaterte opplysninger fra deltakerne, for eksempel ved bekreftelse mv.

Prinsippet om **Lagringsbegrensning**



Lagringsbegrensning

- ▶ Personopplysninger skal ikke lagres lengre enn nødvendig for formålene de behandles for.
- ▶ Når formålet er oppnådd skal opplysningene enten slettes eller anonymiseres
- ▶ Sammenheng med prinsippet om formålsbegrensning
- ▶ Lagring til arkiv-, forskning- og statistikkformål





Tiltak virksomheten kan iverksette for å oppfylle prinsippet om Lagringsbegrensning

- ▶ Tiltak virksomhetene må etablere er sletterutiner som regulerer når opplysningene skal slettes etter at formålet er oppnådd
- ▶ Avsjekk med relevant regelverk som kan regulere lagringstiden, for eksempel Arkivloven, pasientjournallov mv.
- ▶ Eksempel på slike sletterutiner kan være gjennom periodiske gjennomganger av personopplysninger, enten manuelt eller automatisk, eller angi tidsfrister for sletting m.m.

Spørsmål til deltakerne:



Lagringsbegrensing

Har din virksomhet etablert gode sletterutiner?





Lagringsbegrensning

Eksempler:

▶ Saksbehandlingssystem:

- Ved behandling av ansattopplysninger kan virksomheten påse at sletterutiner er på plass ved endring eller opphør av ansattforholdet.
- Ved behandling av personopplysninger knyttet til utførelse av oppgaver i saksbehandlingssystemet kan tiltak for å oppfylle Lagringsbegrensning være:
 - Automatiske sletteintervaller sett opp mot arkivplikten virksomheten har.
 - Manuelle sletterutiner som de ansatte er pålagt å følge aktivt.

▶ Arrangementer:

- Når formål med behandlingen av opplysningene knyttet til arrangementet er oppnådd må opplysningene slettes. Det må derfor etableres sletterutiner slik at virksomheten kan påse at dette blir gjort.
 - Det må tas hensyn til kvalitetsforbedringsformål, statistikkuttrekk evt. annet
- Det er også viktig at det etableres gode sletterutiner dersom en deltaker trekker tilbake sitt avgitte samtykke.

Prinsippet om **Konfidensialitet og Integritet**



Konfidensialitet og integritet

- Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysninger
 - Det betyr: behandles på en måte som sikrer integritet og konfidensialitet
- Dette prinsippet må sees i sammenheng med virksomhetene plikt til å iverksette tekniske og organisatoriske tiltak for:
 - å ivareta krav til internkontrolldokumentasjon,
 - innebygd personvern og personvern som standardinnstilling
 - krav til sikkerhet ved behandling av personopplysninger
 - oppfylle krav ved bruk av databehandler

Tiltak virksomheten kan iverksette for å oppfylle kravet til Konfidensialitet og Integritet



Konfidensialitet og integritet

- ▶ Virksomheten må gjennomføre en risiko- og sårbarhetsanalyse
- ▶ Tiltak mot uautorisert utlevering og tilgang til opplysningene
 - Tilgangskontroll som verifiserer at ansatt er rette vedkommende
- ▶ Tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger
 - Back-up
 - Logg over tilgang og endringer som gjøres i systemet og for å håndtere sikkerhetsbrudd

Spørsmål til deltakerne:



Konfidensialitet og integritet

Vet du hvilke rutiner din virksomheter har etablert for å sikre kravet Integritet og Konfidensialitet?



Eksempler på hvordan virksomheten kan ivareta prinsippet om Konfidensialitet og Integritet



Konfidensialitet og integritet

► Saksbehandlingssystem:

- Tekniske tiltak kan være:
 - Iverksette tiltak som sikrer uautorisert utlevering og tilgang til personopplysninger
 - Tiltak som sikrer back-up
 - Tiltak som sørger for at systemet er robust mot sårbarheter, angrep og uhell
 - Tiltak som etablering av logger for oversikt over bruk, endringer og også rutiner for gjennomgang av disse loggene
- Organisatoriske tiltak kan være:
 - retningslinjer for tildeling av tilganger
 - rutiner for bruk av saksbehandlingssystemet
 - for håndtering av sikkerhetsbrudd mv.

► Arrangementer:

- Tiltak kan være at opplysningene om deltakerne er lagret på et område med begrenset tilgang (tilgangsstyring)
- Rutiner som sikrer at man oppdager endringer i opplysningene





Prinsippet om **Ansvarlighet**

- ▶ Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes.
- ▶ Understreker ansvaret til virksomhetene for å opptre i samsvar med reglene i personvernforordningen



Tiltak som virksomheten kan iverksette for å oppfylle prinsippet om Ansvarlighet

- ▶ Opptre proaktivt
- ▶ Etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre etterlevelse av regelverket
- ▶ Vise at faktisk opptrer i samsvar med reglene ved å dokumentere ansvars plasseringen



Spørsmål til deltakerne:

Vet dere hvem i deres virksomhet som er ansvarlig for behandlingen av personopplysninger?





Eksempler

▶ Saksbehandlingssystem:

- Det overordnede ansvaret vil sannsynligvis være Oslo kommune
- Mens det operative ansvaret vil ligge til den enkelte virksomhetsleder
- Saksbehandlere vil også ha et ansvar for å forholde seg til retningslinjer og sørge for å ivareta virksomhetens behandling av personopplysninger på en god måte

▶ Arrangementer:

- Overordnet ansvar vil også her være Oslo kommune
- Det operative ansvaret vil ved arrangementer være ansvarlig virksomhet ved virksomhetsleder

Har du spørsmål om personvern? Ta kontakt!

Linda:
linda.mari.knutsen@byr.oslo.kommune.no

Maryke:
maryke.nuth@byr.oslo.kommune.no



Takk for oss! 😊

