

Innhold

[1. Om malene 3](#_Toc102391984)

[2. Om veilederen 3](#_Toc102391985)

[3. Til kap. 6 IP (Særlige plikter og unntak etter GDPR art. 35) 4](#_Toc102391986)

[4. Til kap. 7 IP (Grunnleggende informasjon om behov for DPIA) 5](#_Toc102391987)

[5. Til kap. 4 PLM og DPIA (Behandlingens art, omfang og kontekst) 7](#_Toc102391988)

[6. Til kap. 5 PLM og DPIA (Behandlingens formål og begrunnelse) 11](#_Toc102391989)

[7. Til kap. 6 PLM og DPIA (Behandlingens lovlighet) 12](#_Toc102391990)

[8. Til kap. 7 DPIA (Behandlingens nødvendighet og proporsjonalitet) 14](#_Toc102391991)

[9. Til kapitel 8 PLM og DPIA (Risiko og tiltak) 26](#_Toc102391992)

[**Risikoanalyse 26**](#_Toc102391993)

[**Risikomatrise 27**](#_Toc102391994)

**Vedlegg 1** (ikke del av dette dokumentet) – Begrepsliste

**Vedlegg 2** (ikke del av dette dokumentet) – Eksempel på utfylling risikoanalyse personvernrisiko

**Vedlegg 3** (ikke del av dette dokumentet) – Sammenheng mellom IP, PLM og DPIA

# Om malene

FIN/ISI har utarbeidet maler for personvernvurderinger som skal brukes av virksomheter i Oslo kommune. Malene skal bidra til å løfte personvern i kommunen, bedre etterlevelse av personvernregelverket og høyere kvalitet i personvernvurderinger.

Malene inneholder flere spørsmål der virksomhetene skal krysse av for svaralternativer, slik at arbeidet med personvernvurderinger blir mer effektivt.

Det er 3 maler:

**Mal for innledende personvernvurdering (IP)**

IP er ment som en kartlegging av grunnleggende informasjon ved behandlingen, for å sikre at virksomhetene har en slik systematisk beskrivelse på plass. Innholdet i IP vil også være relevant for oversikt over behandling av personopplysninger (behandlingsoversikt/protokoll), personvernerklæringer, ved avvikshåndtering og i kontakt med den registrerte. Noen av de nødvendige vurderinger som må gjøres etter personvernregelverket vil også ivaretas.

**Mal for personvernkonsekvensvurdering ved lav/middels risiko (PLM)**

PLM gjennomføres på bakgrunn av konklusjon i IP som viser at personvernrisikoen ved behandlingen er lav/middels. Hensikten med PLM er å sikre at virksomheten har oversikt over hvilke konsekvenser den planlagte behandlingen vil ha for personvernet, sørge for at de registrertes rettigheter og friheter blir ivaretatt og bidra til at virksomheten etterlever kravene i regelverket for behandling av personopplysninger.

**Mal for personvernkonsekvensvurdering ved høyrisiko (DPIA) med vedlegg**

DPIA gjennomføres på bakgrunn av konklusjon i IP som viser at personvernrisikoen ved behandlingen er høy. DPIA har samme formål som PLM, men er utvidet med større fokus på de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter og risikoreduserende tiltak.

Spørsmålene i malene er utformet ut fra krav i regelverket og kjente og innmeldte behov fra ulike sektorer i Oslo kommune. I tillegg er malene pedagogisk lagt opp på en slik måte at virksomhetene gjør nødvendige vurderinger for å sikre etterlevelse av personvernregelverket uavhengig av risikonivå ved behandling personopplysninger. Spørsmålene i malene er delvis likelydende, men justert basert på risikonivå.

For prosess knyttet til hvordan malene brukes, se «Om vurdering» i alle malene.

Sammenheng mellom innholdet i malene finnes som vedlegg 3 til denne veilederen.

# Om veilederen

Denne veilederen skal bidra til at malene blir brukt konsistent mellom virksomhetene, og i tillegg sikre at nødvendige personvernvurderinger gjennomføres på en god måte.

Veilederen inneholder tolkning eller forklaring av GDPR-krav, vurderingsmomenter og praktiske eksempler fra kommunen. Det henvises til gjeldende veiledere og andre sentrale dokumenter i Oslo kommune, samt til Datatilsynet og EU-kilder.

Veilederen beskriver hvordan de ulike kapitlene i IP, PLM og DPIA skal fylles ut. Innholdet i kapitlene 1-3 i alle malene er i stor grad likt, og disse spørsmålene skal være lette å svare på uten behov for veiledning. Forklaring av begreper som brukes i disse kapitlene finnes i Vedlegg 1. Veilederen inneholder konkret veiledning for de øvrige kapitlene i alle tre malene.

# Til kap. 6 IP (Særlige plikter og unntak etter GDPR art. 35)

Virksomhetene har en plikt til å gjennomføre en DPIA dersom det anses at behandlingen vil medføre høy risiko for brudd på eller svekkelse av de registrertes rettigheter og friheter.

Formålet med denne delen av vurderingen er å kartlegge om virksomheten etter GDPR er pålagt å gjennomføre en DPIA, eller om virksomheten oppfyller kriteriene for unntak fra plikten til å gjennomføre en DPIA. Det er verdt å merke seg at unntaksregelen er snever.

**Plikt til å gjennomføre DPIA ved en behandling**

Virksomheten må vurdere hvert punkt konkret, da bokstav a-c hver for seg gi en plikt til å gjennomføre DPIA etter GDPR art. 35 nr. 3.

Til punkt a):

Det skal gjennomføres DPIA når behandlingen oppfyller alle de følgende kriteriene:

* *Behandlingen er systematisk*. Dette kan f.eks. skje ved kontinuerlig og automatisk innsamling av personopplysninger uten at den registrerte vet om det, eller ved kameraovervåkning.
* *Behandlingen er omfattende*. Dvs. at det må være en viss mengde med personopplysninger av ulik art som behandles om den enkelte, og vil ofte gjelde et stort antall personer. Antall personer må settes i norsk kontekst, og skal ikke sammenlignes med andre europeiske land.
* *Personopplysningene som behandles er av personlig art*. Dette vil ofte være en subjektiv vurdering og må ses på helt konkret. Vurderingsspørsmål kan være om det er typiske opplysninger den registrerte ønsker å holde for seg selv, som ikke er allment kjent, og som den enkelte vanligvis vil kunne velge hvem de vil dele med.
* *Behandlingen er automatisert*. Dette kan for eksempel være profilering med mål om å finne informasjonsmønstre som kan si noe om sannsynlighet for et visst handlingsmønster eller preferanser hos enkeltpersoner.
* *Opplysningene påvirker rettsvirkninger for den enkelte, eller påvirker i betydelig grad:* Dette gjelder når personopplysningene som behandles påvirker om den registrerte mottar en rettighet eller ikke, f. eks. vedtak om rett til skoleskyss eller innvilgelse av sykehjemsplass. Det kan også være innsamling og sammenstilling av personopplysninger for å avgjøre om den registrerte skal få tilbud om, fortsette å motta, eller nektes et produkt, en tjeneste eller et tilbud.

Til punkt b):

Det skal gjennomføres DPIA dersom det planlegges å behandle særlige kategorier av personopplysninger, eller opplysninger om straffedommer og lovovertredelser som kan knyttes til en enkeltperson, i stor skala.

Til punkt c):

Det skal gjennomføres DPIA dersom det planlegges å drive systematisk overvåkning i stor skala, når det foregår i et offentlig tilgjengelig område. Med overvåkning menes at enkeltpersoner registreres, filmes, streames eller monitoreres uten at de har mulighet til å påvirke dette selv. Dette kan f. eks. være sikkerhetskamera på et bibliotek eller en skole, eller et uteområde hvor mange mennesker ferdes.

**Unntak fra plikten til å gjennomføre DPIA**

Unntak fra plikten til å gjøre DPIA gjelder dersom *alle* de tre kriteriene som GDPR art. 35 nr. 10 er oppfylt.

Til punkt a):

Dette unntaket gjelder kun dersom følgende behandlingsgrunnlag er lagt til grunn: behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige (GDPR art. 6 nr. 1 bokstav c), eller behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt (GDPR art. 6 nr. 1 bokstav e).

Disse to behandlingsgrunnlagene krever at behandlingen suppleres av et annet rettslig grunnlag. Se veileder om behandlingsgrunnlag for nærmere beskrivelse av disse to behandlingsgrunnlagene og supplerende rettsgrunnlag.

Til punkt b):

For å kunne bruke dette unntaket b) kreves også at de spesifikke behandlingsaktivitetene fremkommer tydelig i rettsgrunnlagene.

Til punkt c):

Poenget med vurderingen er å undersøke om lovgiver allerede har gjennomført personvernkonsekvensvurderinger som en del av en generell personvernvurdering i forbindelse med vedtakelse av loven. Det anses at slike vurderinger har ivaretatt behovet for vurdering av den registrertes personvern knyttet til behandling av personopplysninger. I Norge er det sjelden at myndigheten gjøre en tilstrekkelige personvernvurderinger i forbindelse med vedtakelse av loven. Dette vil si at unntaket sjelden kommer til anvendelse.

# Til kap. 7 IP (Grunnleggende informasjon om behov for DPIA)

Det skal alltid gjøres en konkret vurdering av behovet for å gjennomføre DPIA sett i lys av risiko for rettighetene og frihetene til den registrerte.

I malen skal virksomhetene svare ja eller nei på en rekke påstander, som til sammen skal hjelpe å gjøre en vurdering av om DPIA må gjennomføres eller ikke, dvs. om det er høy eller lav/middels risiko. Listen er ikke uttømmende, men gir en god indikasjon på når det anses å være høy personvernrisiko. Hver behandling må ses på helhetlig, i lys av personvernprinsippene. En tommelfingerregel, er at det vil være behov for å gjennomføre en DPIA dersom en behandling kan oppleves som inngripende for den enkelte på bakgrunn av typen personopplysninger som skal brukes eller måten de brukes på. Uforutsigbarhet for den enkelte vil også være med å trekke i retning av en DPIA.

|  |  |
| --- | --- |
| Punkt 1 | Se begrepslisten for hvilke opplysninger som omfattes av særlige kategorier. Personopplysninger av følsom karakter for den registrerte er gjerne subjektiv og må konkret vurderes ut fra typen opplysninger i den enkelte behandling. Se begrepslisten for «personopplysninger av følsom karakter». Vurderingsspørsmål kan være om det er typiske opplysninger man ønsker å holde for seg selv, som ikke er allment kjent, og som den enkelte vanligvis vil kunne velge hvem de vil dele med.  |
| Punkt 2  | Se begrepslisten for «stor skala». |
| Punkt 3 | Behandlingen må være noe nytt, som i liten grad eller aldri er gjennomført før, slik at den registrerte ikke antas å kjenne til behandlingen fra før.  |
| Punkt 4 | Eksempel på dette er en behandling som innebærer at det treffes beslutninger om en fysisk persons tilgang til et produkt, en tjeneste, en mulighet eller en fordel. |
| Punkt 5 | Det er gjerne en subjektiv vurdering av hva som anses som inngripende for den enkelte, men virksomheten kan vurdere om det vil være en uventet eller overraskende måte eller form å bli kontaktet på. I noen sammenhenger kan SMS virke inngripende, i andre sammenhenger personlig e-post. Har den registrerte selv oppgitt hvordan de vil kontaktes i sammenhengen, kan det tale for at det ikke vil oppleves som inngripende hvis de blir kontaktet på den oppgitte måten. |
| Punkt 6 | Vurderingsspørsmål her kan være: * Har behandlingen som mål å kartlegge eller finne informasjonsmønstre som kan si noe om sannsynlighet for et visst handlingsmønster eller preferanser hos enkeltpersoner eller grupper?
* Skal informasjonen brukes til å sette personer i ulike grupperinger basert på svar, adferd eller bevegelses- eller handlingsmønster?
 |
| Punkt 7 | Se begrepslisten for «automatisert behandling». Dette gjelder når personopplysningene som behandles påvirker om den registrerte mottar en rettighet eller ikke, f. eks. vedtak om rett til skoleskyss eller innvilgelse av sykehjemsplass. Det kan også være innsamling og sammenstilling av personopplysninger for å avgjøre om den registrerte skal få tilbud om, fortsette å motta, eller nektes et produkt, en tjeneste eller et tilbud. |
| Punkt 8 | Se begrepslisten for «systematisk». Med overvåkning og sporing menes både bruk av kamera/videobilder for å registrere bevegelsesmønstre eller elektroniske spor som kan si noe om nettaktivitet eller tidsbruk på en oppgave. |
| Punkt 9 | Sammenstilling kan skje ved at det er samlet inn personopplysninger for to ulike formål, som deretter skal settes sammen i et system for å gi ny informasjon. For eksempel informasjon om at en person har fått barn settes sammen med informasjon om inntekt, og informasjon samlet brukes til å avgjøre om personen har rett til økonomisk støtte til barnehageplass.  |
| Punkt 10 | Når det gjelder sårbare personer, kan virksomheten vurdere den enkeltes evne til å ivareta egne rettigheter og forstå konsekvensen av den faktiske behandlingen. Relevante vurderingsmomenter kan være aldersgruppe eller helse. Når det gjelder ubalanse i styrkeforhold, kan virksomheten se på den enkeltes mulighet til selvbestemmelse uten press. Vurderingsspørsmål kan være om det er sannsynlig at den registrerte på en enkel måte vil kunne utøve egne rettigheter, f. eks. gi eller trekke tilbake sitt samtykke uten at dette føles ubehagelig. Faktisk frivillighet er et nøkkelord her. Se begrepslisten for eksempler. |
| Punkt 11 | Eksempler på dette er ansiktsgjenkjenning, registrering av kroppens helsetilstand, eller registering av bruk av fysiske ting som kobles på nett (kaffemaskin, strømboks, kjøleskap mm). Bruk av ny teknologi kan føre til personvernkonsekvenser som ikke er tenkt på, eller som er uforutsigbare for den registrerte. |
| Punkt 12 | Eksempler kan være der virksomheter innhenter informasjon andre har samlet inn om den registrerte, f. eks. fra Skatteetaten eller NAV. |
| Punkt 13 | Dette gjelder for behandlinger som skal eller kan rettes mot barn frem til de er 18 år. Det gjelder både for nettjenester og apper som retter seg mot målgruppen, men også for tjenester eller system som behandler personopplysninger om barn i forbindelse med markedsføring. I det offentlige kan dette f. eks. gjelde profilering for å finne ut hvilke barn som skal motta informasjon om fritidstilbud i bydelen.  |
| Punkt 14 | Tredjeland er utenfor EU/EØS som ikke godkjent av EU-kommisjonen som land med tilstrekkelig beskyttelsesnivå for personvernet som EU land.Behandling kan utføres av databehandler eller behandlingsansvarlig, og gjelder også for behandling av personopplysninger via servere i EU/EØS av personer i tredjeland (dvs. at noen i et tredjeland har tilgang, selv om dataen ikke er lagret i tredjelandet).Behandling i tredjeland vil sannsynligvis ha høy risiko og dermed kreve en DPIA. |

# Til kap. 4 PLM og DPIA (Behandlingens art, omfang og kontekst)

1. **Behandlingens omfang**

*Behandlingens omfang* betyr at virksomheten må se på i hvilken utstrekning behandling av personopplysninger forekommer. Personvernregelverket viser til at behandlinger som forekommer i stort omfang også kalles «stor skala». For eksempel kan en behandling omfatte både alminnelige personopplysninger og helseopplysninger (særlige kategorier av personopplysninger), samt IP-adresse til de registrerte. Volumet av data er relativt stort med en viss mengde variabler.

Behandlingen er derimot avgrenset til et lite antall registrerte som oppholder seg i Oslo og opplysningene skal bare innhentes en gang med en kort avgrenset lagringstid. Dette kan det indikerer at behandlingen ikke forekommer i «stor skala».

1. **Behandlingens kontekst**

*Hvilken kontekst behandlingen utføres i* betyr at man må se på hvilken sammenheng behandling av personopplysninger utføres i. Dette kan ha stor betydning for om de registrertes rettigheter og friheter er ivaretatt.

For noen sammenhenger behandles det kun alminnelige personopplysninger og den registrerte har i stor grad kontroll over opplysningene ved at den registrerte avgir disse selv. I andre sammenhenger behandles det mer sensitive personopplysninger (som helseopplysninger) og den registrerte har ingen medbestemmelse i hvilke opplysninger som registreres. I siste eksempel har den registrerte dermed mindre kontroll over sine personopplysninger enn i første eksempel.

For eksempel vil sammenhenger som tilsier at risikoen for den registrertes rettigheter og friheter er høy, være sammenhenger hvor den registrerte har en tydelig forventning om at virksomheten ivaretar den registrertes personvern. Dette kan være de tilfeller man behandler helseopplysninger om en pasient. Pasienten vil da ha en klar forventning om at krav til konfidensialitet blir ivaretatt. Det samme gjelder for arbeidstaker, når arbeidsgiver behandler personopplysninger i arbeidsforholdet, herunder opplysninger om inntekt, barn, personalsaker, sykefravær mv.

Dersom det er ujevnt styrkeforhold mellom den behandlingsansvarlige og den registrerte, skal dette komme frem i vurderingen av behandlingens kontekst. For eksempel vil styrkeforholdet mellom arbeidsgiver og arbeidstaker være skjevt, ettersom arbeidsgiver som følge av sin styringsrett vil kunne pålegge sanksjoner overfor arbeidstaker. Det samme kan gjelder skole og elevforhold, pasient og kommunal helsetilbyder mv.

Det er også viktig å vise til/være bevisst på tilfeller hvor personopplysninger hentes fra ulike datasett eller kilder internt eller utenfor Oslo kommune. Dette fordi en slik behandling kan fremstå som uoversiktlig og uforutsigbart for den registrerte, og det er viktig at man som behandlingsansvarlig oppfyller de plikter som følger av personvernregelverket mht. åpenhet og krav om informasjon til de registrerte. For eksempel vil digitale tjenester på en plattform kunne innhente opplysninger om den registrerte fra administrative systemer, både internt i Oslo kommune som skoleadministrative systemer og eksterne systemer som Folkeregisteret eller nasjonale helseregistre. Dette er ikke naturlig forutsigbart og lett forståelig for den enkelte registrerte, og må tas med i vurderingen av behandlingens kontekst.

1. **Overføring til utlandet**

I GDPR kapittel V oppstilles krav om at all overføring ut av EU/EØS skal ha et særskilt grunnlag for at overføringen til tredjeland er lovlig. Dette kravet kommer i tillegg til kravet om behandlingsgrunnlag etter GDPR art. 6 og art. 9. Det er viktig at virksomheten har identifisert om det finnes et overføringsgrunnlag før personopplysningene overføres til tredjelandet. Hvis det ikke finnes, er overføringen ulovlig.

Godkjente tredjeland[[1]](#footnote-1)

Noen tredjeland er godkjent av EU-kommisjonen ved at de har regler som ivaretar personvernet på en tilsvarende måte som land innad i EU/EØS. Disse er omtalt i GDPR art. 45. Skal personopplysningene overføres til et godkjent tredjeland vil risikoen for den registrertes rettigheter og frihetene ikke anses for å være høy. Dersom det forekommer en overføring til et godkjent tredjeland kan det være tilstrekkelig å gjennomføre en personvernvurdering for lav/middels risiko, men dette avhenger av andre faktorer også.

Ikke-godkjente tredjeland (høy risiko)

Dersom personopplysninger skal overføres til ikke-godkjente tredjeland vil risikoen for den registrertes rettigheter og friheter være høy og en DPIA må gjennomføres. Ved overføring til ikke-godkjente tredjeland stilles det krav om at behandlingsansvarlig skal sørge for «nødvendige garantier» for at overføringen skal være gyldig. I tillegg må overføringen gjøres under forutsetning av at den registrerte har håndhevbare rettigheter og effektive rettsmidler. Dette er regulert i GDPR art. 46.

Det er opp til virksomheten selv å finne ut hva som er riktig overføringsgrunnlag. GDPR oppstiller flere overføringsgrunnlag etter art. 46, men vi har i denne veiledningen trukket frem de mest sentrale for virksomheter i Oslo kommune.

De mest relevante overføringsgrunnlag etter GDPR art. 46 er:

1. **Standard personvernbestemmelser vedtatt av EU-kommisjonen (standard contractual clauses (SCC))**

Dette er det vanligste overføringsgrunnlaget når personopplysninger overføres til ikke-godkjente tredjeland. Ved signering av standard personvernbestemmelser forplikter leverandøren (dataimportøren) seg til å behandle opplysningene i samsvar med de kravene som gjelder innenfor EU/EØS-området. Samtidig må virksomheten/behandlingsansvarlig (dataeksportøren), sjekke at personopplysningene som blir overført, faktisk får tilstrekkelig beskyttelsesnivå på lik linje som i EU/EØS før overføringen. I tillegg plikter virksomheten/behandlingsansvarlig å sikre at rettssystemet i mottakerlandet gjør det mulig å følge de standard personvernbestemmelsene i praksis. Leverandøren plikter å informere virksomheten/behandlingsansvarlig så raskt som mulig om eventuelle hindringer for å oppfylle kravene. Dersom man bruker disse personvernbestemmelsene uendret, trenger man verken søke om forhåndsgodkjenning eller varsle Datatilsynet. Man kan også innta standard personvernbestemmelsene i en større avtale, samt føye til klausuler så fremt disse ikke er i motstrid (direkte eller indirekte) med standard personvernbestemmelser vedtatt av EU-kommisjonen.

Dersom man benytter overføringsgrunnlag etter GDPR art. 46 og man ikke er trygg på at beskyttelsesnivået i tredjelandet i praksis vil være likestilt med EU/EØS sitt beskyttelsesnivå, må også ytterligere tiltak iverksettes. Dette fordi krenkelse av personvernet må motvirkes. Tiltakene kan være tekniske, juridiske eller organisatoriske. Tekniske tiltak bør som utgangspunkt alltid inkluderes, da lokale lover i tredjelandet går foran overføringsgrunnlaget (som ofte er en juridisk bindende avtale) og da vil ytterligere juridiske tiltak kanskje ikke være aktuelt. Men hva som er effektivt i praksis må vurderes konkret i hver enkelt sak.

Tekniske tiltak kan for eksempel være kryptering eller pseudonymisering, men også andre tekniske tiltak kan være aktuelt. Juridiske tiltak kan for eksempel være kontraktsmessig forpliktelse til å iverksette bestemte tekniske tiltak og tiltak når det gjelder nøkkelhåndtering. Organisatoriske tiltak kan gjerne være rutiner, fremgangsmåter og internkontroll for virksomheten. Dette er for eksempel viktig dersom virksomheten får utleveringsbegjæring. Har man gode rutiner for håndtering av slike forespørsler er det viktig med gode rapporteringslinjer og dokumentasjon mv. Dette gjelder også for leverandøren.

For mer informasjon om standard personvernbestemmelser og tilleggskravene i lys av Schrems II, se Datatilsynets veileder om overføring til tredjeland.[[2]](#footnote-2)

1. **Bindende virksomhetsregler (binding corporate rules (BCR))**

Dette er interne regler for overføring av personopplysninger i multinasjonale selskaper, et konsern eller en gruppe av foretak som utøver en felles økonomisk virksomhet.

En godkjent BCR tillater multinasjonale selskaper å overføre personopplysninger internasjonalt innenfor samme konserngruppe til land som ikke gir et tilstrekkelig beskyttelsesnivå for personopplysninger. Det er Datatilsynet som kan vedta disse etter søknad og en godkjenningsprosess, samt en uttalelse fra Personvernrådet.

Dersom dette overføringsgrunnlaget er aktuelt for en virksomhet i Oslo kommune må flere vilkår oppfylles. For nærmere informasjon, se Datatilsynets veileder om overføring av personopplysninger til tredjeland, kapittel 5.[[3]](#footnote-3)

* Standard personvernbestemmelser vedtatt av tilsynsmyndighet og godkjent av EU-kommisjonen

Dette er personvernbestemmelser som Datatilsynet selv kan vedta og som må godkjennes av EU-kommisjonen. Per dags dato finnes det ingen presedens og godkjenningsprosessen vil være tidkrevende.

Merk at GDPR art. 46 oppstiller også andre alternative overføringsgrunnlag som virksomheten kan ta stilling til ved vurdering av overføring til ikke-godkjente tredjeland.

# Til kap. 5 PLM og DPIA (Behandlingens formål og begrunnelse)

1. **Formål for førstegangsbehandling**

Formålet med behandling av personopplysningene er hva opplysningene skal brukes til, dvs. hensikten eller planen med innsamlingen av opplysningene. Formålsbeskrivelsen må være dekkende for alle behandlingsaktiviteter som er planlagt for å oppnå formålet. Formålet bør være detaljert og tydelig nok til å dekke kravet om at formålet skal være spesifikt og uttrykkelig angitt. Formålet må altså være konkret og presist beskrevet, men likevel omfatte det virksomheten planlegger å bruke personopplysningene til. Formålet med behandlingen må i tillegg være berettiget, dvs. at det må være rimelige grunner til at virksomheten skal behandle personopplysningene. Merk at det kan være snakk om flere behandlingsaktiviteter med ulike formål.

Det må skilles mellom egne og andres formål. Dette kan være særlig aktuelt når samme system brukes av flere virksomheter i kommunen der hver virksomhet har sine egne formål med bruken. Det er behandlingsansvarlig som har plikt til å gjennomføre DPIA ved høy risiko. Behandlingsansvarlig er den som blant annet bestemmer formålet med behandlingen. Skillet mellom egne og andres formål med behandlingen har derfor betydning både for *hvem* som skal gjennomføre DPIA (behandlingsansvarlig) og *hva* det skal gjennomføres en DPIA av (eget formål). Husk at de utførende oppgavene ved behandlingsansvaret ofte kan være delegert til noen andre enn den som har det faktiske (juridiske) behandlingsansvaret.

Et eksempel på formålet med en behandling kan være fordeling av kommunale boliger.

Overordnet formål med behandlingen er en riktig og rettferdig fordeling av kommunale boliger i Oslo kommune.

Behandlingen til dette formålet innebærer flere behandlingsaktiviteter med ulike underliggende formål, som f. eks:

* Formålet med innsamlingen av personopplysninger er å ha nok informasjon til å kunne fatte vedtak om brukeren har krav på kommunal bolig eller ikke.
* Formålet med lagringen og sammenstillingen med folkeregisteropplysninger, er for å kunne følge opp brukeren så lenge vedkommende bor i kommunal bolig.
* I tillegg brukes personopplysningene til analyse og statistikk for å styre og forbedre tjenesten, og for å sikre at kommunen når sine mål om en rettferdig fordeling av kommunale boliger.
1. **Formål ved viderebehandling**

Når personopplysninger som tidligere er samlet inn for et annet formål skal viderebehandles, beskrives både det nye formålet og det opprinnelige formålet med behandlingen. Formålsbeskrivelsene skal også brukes til å finne ut om det nye formålet er forenlig med det opprinnelige formålet. Hvis det nye formålet er uforenlig med det opprinnelige formålet kan ikke personopplysningene behandles for det nye formålet, men kun for opprinnelig formål. Se Veileder om behandlingsgrunnlag kap.4.2 s.13-15 for hjelp til vurderingen av om nytt og opprinnelig formål er forenlige.

Et eksempel på viderebehandling kan være ifbm adgangskontroll på en arbeidsplass.

* Opprinnelig formål med innsamlingen av personopplysninger i adgangskontroll med kort som skannes når man kommer og går (herunder pauser), er å ivareta fysisk sikkerhet og sikre at kun autoriserte ansatte kan komme inn i hovedbygget på en byggeplass. Behandlingen av personopplysninger skjer også for å holde en oversikt over hvilke ansatte som er på jobb i forbindelse med HMS-arbeid hvis det skulle skje en hendelse.
* Det nye formålet er å behandle personopplysningene fra adgangskontrollen for å lette arbeidet med timeføringen for ansatte som jobber på byggeplassen. Det nye formålet her vil være uforenlig med den opprinnelig formålet som handler om å ivareta sikkerheten på byggeplassen.

**C. Begrunnelse for formålet** [gjelder kun DPIA]

I DPIA skal i tillegg formålet med behandlingen begrunnes, for å kunne gjøre en nødvendighets- og proporsjonalitetsvurdering. Her må virksomheten angi hva de ønsker å oppnå med behandlingen, samt fordeler og ulemper. Ut fra dette skal de gjøre en vurdering av om formålet er forholdsmessig.

# Til kap. 6 PLM og DPIA (Behandlingens lovlighet)

1. **Behandlingsgrunnlag**

Når det er snakk om større prosjekter bør virksomhetene innhente bistand fra jurist eller lignende med personvernkompetanse.

All behandling av personopplysninger krever et rettslig grunnlag for å være lovlig, dette kalles ofte behandlingsgrunnlag. Det finnes flere behandlingsgrunnlag i GDPR art. 6 nr.1, f. eks. samtykke, rettslige forpliktelse (f. eks. lovpålagte oppgaver i kommunen), avtale mv. Hvis det skal behandles særlige kategorier (sensitive) personopplysninger, kreves det at virksomheten også har et behandlingsgrunnlag som regnes som et unntak etter GDPR art. 9 nr. 2. Husk at det er mange forbehold ved bruk av behandlingsgrunnlagene etter GDPR art. 9 nr. 2, så det er viktig å sette seg godt inn i bestemmelsen før den brukes.

Husk også at noen av behandlingsgrunnlagene både i GDPR art. 6 og art. 9 krever supplerende rettsgrunnlag. Supplerende rettsgrunnlag betyr at behandlingen må ha et ekstra rettsgrunnlag i den nasjonale lovgivningen. Det finnes noen generelle supplerende rettsgrunnlag i personopplysningsloven §§ 6-9. I tillegg vil det finnes supplerende rettsgrunnlag både i generell særlovgivning som f. eks i arkivlova og i sektorlovgivning som f. eks sosialtjenesteloven som gir kommunen konkrete lovpålagte oppgaver. Husk at det ikke trenger å stå konkret i bestemmelsen i den nasjonale lovgivningen at det skal behandles personopplysninger, men behandlingen av personopplysninger må likevel være nødvendig for å kunne oppfylle den rettslige forpliktelsen som ligger i bestemmelsen, som i eksempelet nedenfor.

Et eksempel kan være når kommunen skal behandle personopplysninger for å kunne tildele kommunale boliger. Her vil f. eks behandlingsgrunnlaget være GDPR art. 6 nr. 1 bokstav c) (rettslig forpliktelse), fordi det er snakk om en lovpålagt oppgave for kommunen. Denne bestemmelsen krever et supplerende rettsgrunnlag i nasjonal lovgivning, som her vil være helse- og omsorgstjenesteloven § 3-7, som pålegger kommunen å skaffe bolig til personer som ikke selv kan ivareta sine interesser på boligmarkedet. I helse- og omsorgstjenesteloven § 3-7 står det ikke noe om behandling av personopplysninger i lovbestemmelsen, men det er nødvendig å behandle personopplysninger for å kunne utføre den lovpålagte oppgaven. I dette tilfellet er det i tillegg grunn til å tro at det skal behandles særlige kategorier personopplysninger, f. eks. opplysninger om brukerens helse for å kunne finne riktig bolig. Behandlingsgrunnlag etter GDPR art. 9 kan f. eks være nr. 2 bokstav h) yting av helse- og sosialtjenester.

*Nærmere om berettiget interesse*

Ved bruk av berettiget interesse som behandlingsgrunnlag, kreves det at virksomheten må gjennomføre en interesseavveiing mellom virksomhetens berettigede interesse og den registrertes interesser, grunnleggende rettigheter og friheter, særlig når det er snakk om barn. Virksomheten må veie sin egen interesse i behandlingen opp mot personvernkonsekvensene for den registrerte, og i sum må det være en forholdsmessighet mellom personverninngrepet og den berettigede interessen.[[4]](#footnote-4)

Et annet eksempel kan være bruk av saksbehandlingssystem i kommunen.

Kommunen som arbeidsgiver må behandle noen få personopplysninger om den enkelte ansatte som bruker et saksbehandlingssystem, for å kunne opprette profiler og gi riktige tilganger. Det må gjøres en interesseavveiing mellom kommunens interesse i å behandle personopplysningene og personverninngrepet det utgjør for de ansatte. Saksbehandlingssystemet er et viktig verktøy i kommunens oppgaver, og det vil ikke være mulig å bruke verktøyet uten at det skilles på ansatte som skal ha tilgang og er videre nødvendig for å fordele oppgaver. Personverninngrepet for den ansatte er ikke spesielt stort, det er noen få personopplysninger som behandles, som navn, stillingstittel, epost og telefonnummer. Dette må være innenfor det som forventes i et arbeidsforhold. Det kan derfor sies at kommunen har en berettiget interesse i å behandle personopplysninger om ansatte for å kunne bruke saksbehandlingssystemet.

I DPIA skal det begrunnes hvorfor det aktuelle behandlingsgrunnlaget er valgt.

1. **Samtykke**

For at et samtykke skal være gyldig må alle kravene i GDPR art. 4 nr. 11 og art. nr. 7 være oppfylt, spørsmålene om samtykke i DPIA-malen er dekkende for dette.

Husk at samtykke ikke alltid kan brukes som behandlingsgrunnlag. Det kan f. eks være vanskelig for en arbeidsgiver å oppfylle kravet til et frivillig samtykke pga. at styrkeforholdet mellom behandlingsansvarlig (arbeidsgiver) og den registrerte (arbeidstaker) må vurderes for å finne ut om samtykket er frivillig. Se Veileder om behandlingsgrunnlag for mer informasjon om krav til samtykke.

Et eksempel kan være når kommunen opptrer som offentlig myndighet og fatter vedtak om tildeling av tjenester. I et slikt tilfelle vil den registrerte være i et avhengighetsforhold til kommunen. Samtykket kan derfor ikke ansees som frivillig og kan ikke brukes som behandlingsgrunnlag.

# Til kap. 7 DPIA (Behandlingens nødvendighet og proporsjonalitet)

1. **Nødvendighetsvurdering**

Det skal vurderes om behandlingen slik den er beskrevet kan gjennomføres på en annen eller mindre inngripende måte.

**Om det faktiske formålet med behandlingen oppnås**

Virksomheten bør vurdere hvorvidt behandlingen av personopplysningene vil føre til den ønskede effekt med behandlingen.

Eksempel: Virksomheten skal arrangere et seminar for de ansatte. Arrangøren har behov for å vite antall personer som skal delta på seminaret. Formålet med behandlingen er å finne passende lokaler, få oversikt over hvor mange som skal spise lunsj mv. Som følge av at arrangøren må oppfylle krav til brannsikkerhet, må virksomheten også samle inn og videreformidle oversikt over navn på deltakere. Effekten av denne behandlingen vil være at arrangøren kan tilrettelegge for arrangementet for virksomheten.

**Om formålet kan oppnås uten at personopplysninger behandles**

Virksomheten bør vurdere om ønskede effekt med behandlingen av personopplysningene kan oppnås uten at det behandles personopplysninger.

Eksempel: Ved påmelding til seminar i regi av virksomheten blir de ansatte ofte bedt om å oppgi ulik informasjon som for eksempel navn, alder, e-postadresse, og organisatorisk tilhørighet. Formålet med å samle inn personopplysninger om de ansatte er å finne passende lokaler, få en oversikt over hvor mange som skal spise lunsj mv. I dette tilfellet kan virksomheten oppnå formålet med behandlingen uten å samle inn flere opplysninger enn de ansattes navn.

**Om det finnes andre eller mindre inngripende måter å behandle personopplysningene på**

Virksomheten bør vurdere om finnes andre eller mindre inngripende måter å behandle personopplysningene på.

Eksempel: Ved påmelding til seminar kan de ansatte også bli bedt om å oppgi informasjon om eventuelle hensyn som skal tas under måltider, for eksempel allergier og graviditet. I slike tilfeller kan virksomheten unnlate å be de ansatte om å informere om eventuelle hensyn og heller informere restaurantene om at de må tilrettelegge for eventuelle hensyn samt gi de ansatte informasjon om at de må ta ansvar for å ivareta egne behov.

1. **Proporsjonalitetsvurdering**

I en proporsjonalitetsvurdering må virksomheten vurdere om det er et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordelene som oppnås ved behandlingen av personopplysninger.

Virksomheten må vurdere om behandlingsaktivitetene er i rimelig forhold til formålene.

Eksempel: Virksomheten ønsker å ta i bruk lydopptak i forbindelse med intervju av barn på barnevernsinstitusjon med det formål å kartlegge effekten av et nytt behandlingstilbud på institusjonen. Lydopptak er å anse som en inngripende form for behandling av personopplysninger og for dette tilfellet gjelder det opptak av samtaler med barn, som er å anse som en sårbar gruppe.

I tillegg til at formålet med intervjuet kan oppnås på andre måter enn ved bruk av lydopptak, for eksempel ved å skrive notater og referater, er det ikke et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordelene som oppnås ved behandlingen.

1. **Ivaretakelse av personvernprinsippene**

Personvernprinsippene gir på ulike måter uttrykk for at behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket. Tiltak må iverksettes for å sikre at behandlingen er i henhold til hvert av prinsippene.

**Lovlighet, rettferdighet og åpenhet**

At behandlingen av personopplysninger må være lovlig innebærer først og fremst at det må finnes et rettslig grunnlag for en planlagt behandling av personopplysninger.

At behandlingen av personopplysninger må skje rettferdig betyr at den skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte og ikke foregå på skjulte eller manipulerende måter.

Åpenhet betyr i denne sammenheng at bruken av personopplysninger skal være oversiktlig og forutsigbar for den opplysningene gjelder. Personer det behandles opplysninger om, skal være informert om behandlingen. Åpenhet bidrar til å skape tillit og det setter enkeltpersonen i stand til å bruke sine rettigheter og ivareta sine interesser.

Under dette prinsippet kan virksomheten vurdere:[[5]](#footnote-5)

*Lovlig*

* Finnes det et rettslig grunnlag for den planlagte behandlingen av personopplysningene?
* Er det skille mellom hvilke opplysninger som er nødvendig å behandle for å levere tjenesten, og hvilke andre opplysninger det kan være valgfritt å oppgi for å få tilgang til utvidede tjenester?
* Dersom det behandles sensitive personopplysninger, er minst ett av vilkårene i GDPR art. 9 nr. 2 oppfylt?

*Rettferdig*

* Gjøres behandlingen av personopplysningene i respekt for de registrertes interesser og rimelige forventninger?
* Er behandlingen åpen og forståelig for de registrerte (den skal ikke foregå på fordekte eller manipulerende måter)?
* Er det iverksatt tiltak som gjør resultater fra automatiserte avgjørelser forutsigbare og forståelige?

*Åpenhet*

* Er bruken av personopplysningene oversiktlig og forutsigbar for de opplysningene gjelder?
* Har virksomheten funksjonalitet for å gi informasjon om hvilke opplysninger som behandles, hva de brukes til og mulighet for de registrerte til å gjøre seg kjent med sine rettigheter og hvordan de skal utøve disse?
* Har virksomheten en personvernerklæring på virksomhetens nettsider med generell informasjon om hvordan virksomheten behandler personopplysninger?

**Formålsbegrensning**

Prinsippet innebærer at personopplysninger kun skal behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist, og at alle formål skal være forklart på en måte som gjør at alle berørte har samme forståelse av hva personopplysningene skal brukes til.

At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag, også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenlig med det opprinnelige formålet.

Under dette prinsippet kan virksomheten vurdere:[[6]](#footnote-6)

* Er ethvert formål med behandling av personopplysninger identifisert og presist beskrevet for alle berørte?
* Har formålet med behandlingen et rettslig grunnlag?
* Er formålet i samsvar med de øvrige etiske og rettslige samfunnsnormer?
* Hvis personopplysninger skal gjenbrukes, er behandlingen lovfestet eller er det innhentet nytt samtykke?

**Dataminimering**

Prinsippet om dataminimering innebærer å begrense behandling av personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen.

Under dette prinsippet kan virksomheten vurdere:[[7]](#footnote-7)

* Er alle personopplysningene som behandles relevante og nødvendige for å realisere formålet med behandlingen?
* Kan formålet med behandlingen med rimelighet oppfylles på annen måte enn å behandle personopplysninger? (I så fall skal det ikke innhentes personopplysninger).
* Innhentes det personopplysninger om flere personer enn nødvendig?

**Riktighet**

Prinsippet innebærer at personopplysninger som behandles skal være korrekte, og skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for å straks slette eller rette personopplysninger som er uriktige.

Under dette prinsippet kan virksomheten vurdere:[[8]](#footnote-8)

* Er det iverksatt tiltak som sørger for at personopplysningene er korrekte og oppdaterte (for eksempel tekniske tiltak)?
* Er det iverksatt tiltak som sikrer at personopplysninger som er uriktige med hensyn til formålene de behandles for, straks slettes eller korrigeres?
* Er det iverksatt tiltak som sikrer gjennomgang med hensyn til nødvendig korrigering dersom back-up brukes for gjenoppretting av data?

**Lagringsbegrensning**

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

Under dette prinsippet kan virksomheten vurdere:[[9]](#footnote-9)

* Er det innført tidsfrister for sletting eller periodisk gjennomgang for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig?

**Integritet og konfidensialitet**

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Dette betyr at den behandlingsansvarlige må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.

Under dette prinsippet kan virksomheten vurdere:[[10]](#footnote-10)

* Har behandlingen tiltak mot uautorisert utlevering og tilgang til personopplysninger?
* Har behandlingen som standard å sørge for at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning?
* Har behandlingen tiltak for å spore endringer som gjøres i systemet og for å kunne håndtere sikkerhetsbrudd?
* Har behandlingen tiltak for å sikre at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell?

**Ansvarlighet**

Prinsippet om ansvarlighet understreker den behandlingsansvarliges ansvar for å opptre i samsvar med reglene for behandling av personopplysninger.

Under dette prinsippet kan virksomheten vurdere:[[11]](#footnote-11)

* Opptrer virksomheten proaktivt?
* Har virksomheten etablert alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid?
* Er det dokumentert at virksomheten faktisk opptrer i samsvar med reglene?
1. **Ivaretakelse av de registrertes rettigheter**

Hver enkelt virksomhet har en plikt til å ivareta de registrertes rettigheter når virksomheten samler inn og bruker personopplysninger om enkeltpersoner.

**Rett til informasjon**

Virksomhetene har en plikt til å gi informasjon til den registrerte ved behandling av personopplysninger.

Det stilles også krav til hvordan virksomheten kommuniserer med enkeltpersoner. Regelverket krever at virksomheten skal kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.

Under dette spørsmålet kan virksomheter vurdere:

* Har virksomheten informert de registrerte om at det behandles personopplysninger om dem?
* Har virksomheten tilpasset informasjonen til målgruppen og tatt hensyn til at informasjonen eventuelt er rettet mot barn?
* Har virksomheten adskilt informasjon om behandlingen mot annen informasjon?
* Har virksomheten informert om hvilke tekniske tiltak som er iverksatt for å ivareta hensynet til personvernet?

**Rett til innsyn**

Den registrerte har rett til innsyn i egne personopplysninger. GDPR art. 15 bokstav a-h angir hvilken informasjon den registrerte skal gis ved krav om innsyn.

Under dette spørsmålet kan virksomheten vurdere:[[12]](#footnote-12)

* Er det etablert rutiner for håndtering av krav om innsyn fra den registrerte?
* Besvares et krav om innsyn i egne personopplysninger med informasjon om hvilke konkrete personopplysninger virksomheten behandler om den registrerte, hvordan personopplysningene om den registrerte behandles og hvor opplysningene er hentet fra?

**Rett til retting**

Den registrertes rett til retting innebærer at den registrerte kan kreve retting av uriktige personopplysninger om seg selv og en rett til å få ufullstendige personopplysninger om seg komplettert, herunder ved å fremlegge en framlegge en supplerende erklæring.

Virksomheten skal utføre retting uten ugrunnet opphold og normalt senest innen én måned.

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert rutiner for håndtering av krav om retting fra den registrerte?
* Er det lagt til rette for at den registrerte kan kreve at uriktige opplysninger om seg rettes og at den registrerte kan kreve at ufullstendige opplysninger om seg suppleres?
* Dersom virksomheten har levert ut uriktige eller ufullstendige opplysninger til noen andre, er det lagt til rette for at mottakerne av opplysningene informeres om rettingen?

**Rett til sletting**

I enkelte tilfeller kan de registrerte kreve at egne personopplysninger slettes. Retten til sletting kalles også noen ganger «retten til å bli glemt». De registrertes rett til sletting gjelder imidlertid ikke dersom lagring av opplysningene er nødvendig:

* For å utøve retten til ytrings- og informasjonsfrihet
* For å oppfylle en rettslig forpliktelse som Oslo kommune er underlagt, eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet
* For visse typer bruk innen helsetjenester
* For arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål
* For å fastsette, gjøre gjeldende eller forsvare rettskrav

Virksomheten må være bevisst på at personopplysninger skal slettes dersom det ikke lenger er et nødvendig grunnlag for å lagre opplysningene. Dette skal virksomheten vurdere av eget tiltak eller dersom den registrerte ber om sletting.

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert rutiner for håndtering av krav om sletting?
* Er det lagt til rette for at den registrerte kan kreve at personopplysninger om seg slettes?
* Er det lagt til rette for at virksomheten sletter personopplysninger dersom det ikke lenger er et nødvendig grunnlag for å lagre opplysningene?

**Rett til begrensning**

Retten til begrensning innebærer at den registrerte i noen tilfeller kan be om at måten virksomheten bruker personopplysningene til den registrerte på, begrenses. I så fall kan den registrertes personopplysninger lagres, men ikke behandles utover dette uten den registrertes samtykke. Retten til begrensning av behandling av de registrertes personopplysninger gjelder ikke dersom fortsatt behandling av personopplysningene er nødvendig:

* For å fastsette, gjøre gjeldende eller forsvare rettskrav
* For å verne en annen fysisk eller juridisk persons rettigheter
* Av hensyn til viktige allmenne interesser

Virksomheten skal sørge for begrensning uten ugrunnet opphold og normalt senest innen én måned.

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert rutiner for å håndtere krav om begrensning av behandling av personopplysninger?
* Er det sikret en teknisk mulighet for å flytte opplysninger til et annet sted (der personopplysninger kun lagres) samtidig som personopplysningene gjøres utilgjengelige for brukere av internett?

**Rett til å protestere**

Den registrertes rett til å protestere innebærer at den registrerte i noen tilfeller kan protestere mot at egne personopplysninger behandles.

Retten til å protestere gjelder ikke i følgende tilfeller:

* Behandling av personopplysningene er nødvendige for å utføre en avtale den registrerte har med virksomheten
* Virksomheten er pålagt i lov å behandle den registrertes personopplysninger
* Behandling av personopplysningene er nødvendig for å utføre en oppgave i allmennhetens interesse

Det fremgår av GDPR art. 21 nr. 1 at den registrerte til enhver tid har rett til å protestere mot behandling av personopplysninger om seg som har grunnlag i blant annet GDPR art. 6 nr. 1 bokstav e).

Virksomheten skal svare på protesten uten ugrunnet opphold og normalt senest innen én måned.

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert gode rutiner for å håndtere protest mot behandling av personopplysningene fra den registrerte?
* Er virksomheten bevisst på at retten til å protestere knytter seg til selve behandlingen av sine personopplysninger og til de konkrete personopplysningene?
* Er det lagt til rette for at den registrerte alltid kan protestere dersom formålet med personopplysningene er direkte eller tilpasset markedsføring?

**Rett til dataportabilitet**

Den registrertes rett til dataportabilitet innebærer:

* Den registrerte har rett til å få utlevert personopplysningene sine og å lagre disse på en privat enhet til videre og personlig bruk.
* Den registrerte har rett til å flytte, kopiere eller overføre personopplysningene sine fra en virksomhet til en annen.

Den registrerte har rett til dataportabilitet dersom:

* behandlingen er basert på samtykke i henhold til GDPR art. 6 nr. 1 bokstav a) eller art. 9 nr. 2 bokstav a) eller en avtale i henhold til art. 6 nr. 1 bokstav b), **og**
* behandlingen utføres automatisk

Rett til dataportabilitet gjelder kun for opplysninger som den registrerte bevisst og aktivt har gitt fra seg og for opplysninger som er samlet inn fra den registrerte gjennom den registrertes aktive bruk av en tjeneste. Retten til dataportabilitet kan bare utøves så fremt den ikke krenker andres registrertes rettigheter og friheter.

Virksomheten skal sørge for begrensning uten ugrunnet opphold og normalt senest innen én måned.

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert gode rutiner for å håndtere krav om dataportabilitet fra den registrerte?
* Er virksomheten bevisst på at retten kun knytter seg til personopplysninger som den registrerte selv har gitt virksomheten og ikke til personopplysninger som ikke er samlet direkte fra den registrerte?
* Vil utøvelse av retten krenke andre registrertes rettigheter eller friheter?

Rett til dataportabilitet vil gjelde i et begrenset omfang i kommunen, da vilkårene for å kunne utøve retten i få tilfeller vil foreligge.

**Rett til å ikke være gjenstand for automatiserte avgjørelser**

Den registrertes rett til å ikke være gjenstand for automatiserte avgjørelser innebærer en rett til å ikke være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, når avgjørelsen har rettsvirkning eller i betydelig grad påvirker den registrerte.

Retten til å ikke være gjenstand for automatiserte avgjørelser gjelder ikke dersom avgjørelsen:

* Er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og virksomheten
* Er tillatt i henhold til unionsretten og eller nasjonal rett og der det også er fastsatt egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser, eller
* Er basert på den registrertes uttrykkelige samtykke

Under dette spørsmålet kan virksomheten vurdere:

* Er det etablert gode rutiner for å håndtere krav om å ikke være gjenstand for automatiserte avgjørelser fra den registrerte?
* Foretar virksomheten automatiserte avgjørelser om de registrerte som har rettsvirkning eller i betydelig grad påvirker den registrerte?
* Dersom retten til å ikke være gjenstand for automatiserte avgjørelser gjelder, har virksomheten gjennomført egnede tiltak for å verne de registrertes rettigheter og friheter og berettigede interesser? Og kan retten til menneskelig inngripen, til å uttrykke sine synspunkter og til å motsette seg avgjørelsen, ivaretas?

Rett til å ikke være gjenstand for automatiske avgjørelser vil gjelde i et begrenset omfang i kommunen, da det kun er store og viktige avgjørelser som er omfattet av denne rettigheten.

1. **Ivaretakelse av de registrertes friheter**

Her skal virksomheten dokumentere at behandlingen er vurdert opp mot sentrale menneskerettigheter som er gjenspeilet i konvensjoner som Norge er bundet av internasjonalt.

**Rett til respekt for privatliv og familieliv, hjem og kommunikasjon**

Her skal virksomheten gjøre en vurdering av om behandlingen medfører at enkeltpersoner utsettes for vilkårlig innblanding. Når det gjelder retten til privatliv, skal den enkelte beskyttes mot vilkårlig publisitet slik at fysisk og psykisk integritet, personlig identitet og personlig informasjon er beskyttet.

Når det gjelder korrespondanse eller kommunikasjon i det offentlige, kan ivaretakelse av frihetene være utfordrende i lys av reglene om offentlighet. Det er spesielt viktig å se offentlig regelverk og grunnleggende menneskerettighet i sammenheng, idet flere hensyn skal ivaretas. I et personvernperspektiv, skal det ikke samles inn mer enn det virksomheten har behov for, noe som kan være utfordrende med tanke på å ivareta ytringsfrihet og unngå sensur. Videre skal ikke korrespondanse deles utover de med et faktisk behov, samtidig som vi skal sikre åpenhet i forvaltningen. Det gjelder å finne balansegangen og gode løsninger som ivaretar rettigheter og plikter på tvers av regelverk.

Under dette spørsmålet kan virksomheten vurdere:

* Vil behandlingen medføre at personopplysninger publiseres eller vises for andre som ikke har et faktisk behov for å se opplysningene?
* Vil behandlingen medføre at det samles inn personopplysninger som en kan regne med den enkelte vil holde for seg selv? Er det i tilfelle nødvendig med innsamling og behandling av slike opplysninger?
* Dersom det er vurdert at kommunikasjon i løsningen er nødvendig, er det mulig å minimere korrespondansen til det som er nødvendig (f.eks. unngå fritekst)?
* Dersom løsningen legger opp til korrespondanse med den registrerte, gjøres dette på en måte som hindrer unødvendig sensur av innholdet?

**Rett til å ikke bli diskriminert**

Overordnet handler dette om et forbud mot enhver forskjellsbehandling på grunnlag av kjønn, rase, hudfarge, etnisk eller sosial opprinnelse, genetiske egenskaper, språk, religion eller tro, politiske eller andre meninger, tilknytning til en nasjonal minoritet, eiendom, fødsel, funksjonshemning, alder eller seksuell orientering. Unntaket er der det finnes et grunnlag for lovlig forskjellsbehandling, f. eks. gjennom lovgivning. I behandling av personopplysninger skal virksomheten sikre at det ikke foregår noen form for urettmessig diskriminering.

Under dette spørsmålet kan virksomheten vurdere:

* Behandles personopplysninger om kjønn, rase hudfarge, etnisitet, sosial opprinnelse, genetiske egenskaper, språk, religion, tro, politiske eller andre meninger, eiendom, funksjonsnedsettelse eller seksuell orientering?
* Hvis ja, innebærer behandlingen er en risiko for at enkelte personer og grupper gis uforholdsmessige privilegier fremfor andre på bakgrunn av personopplysningene som er registrert?

**Ytringsfrihet**

Ytringsfrihet er den friheten den enkelte har til å ytre seg (eller å la være) ved å gi uttrykk for det de mener og ønsker å si noe om. Ytringsfriheten er begrenset av forbud mot å fremsette trusler, ærekrenkelser, privatlivskrenkelser, trakassering og grovt pornografiske, diskriminerende og hatefulle utsagn. Det å stanse en ytring før den fremsettes, er derimot som hovedregel ikke tillatt.

For å beskytte ytringsfriheten, kan ikke kommune begrense eller gripe inn i den enkeltes ytringsfrihet. I et personvernperspektiv, skal virksomheten allikevel sikre at det ikke behandles personopplysninger, herunder også ytringer, som ikke er nødvendige for å oppnå formålet med en behandling. F. eks. kan det lages ferdigdefinerte alternativ til valg fremfor fritekstfelt i et klageskjema.

Under dette spørsmålet kan virksomheten vurdere:

* Er det aktuelt å hindre eller minimere den enkeltes rett til å ytre seg i virksomhetens behandling?
* Hvis ja, finnes det personvernhensyn eller unntaksregler som er lagt til grunn?

**Tanke- tros- og religionsfrihet**

Denne friheten gir en frihet til å gi uttrykk for sin religion, tro, gjerning, utøvelse og etterlevelse av denne. Friheten kan bare begrenses dersom det er nedfelt i lov, det er nødvendig for å beskytte den offentlige sikkerhet, orden, helse eller moral, eller for å beskytte andres rettigheter og friheter. Friheten har paralleller til forbudet mot diskriminering, også i strafferettslig forstand.

Under dette spørsmålet kan virksomheten vurdere:

* Innebærer behandlingen opplysninger om den enkeltes religion eller annen tro?
* Hvis ja, hvordan ivaretas den enkeltes rett til å utrykke dette?
* Hvis ja, hvordan sikres det at den enkeltes frihet ikke innskrenkes?

**F. Databehandlere**

For definisjon av databehandler, se begrepslisten.

Databehandler

En behandlingsansvarlig kan inngå avtale med én eller flere databehandlere. I tilfeller hvor databehandleren inngår avtale med flere databehandlere vil de ulike databehandlerne ha ansvar for ulike deler av behandlingen av personopplysninger.

En databehandler må ikke forveksles med en underdatabehandler. En underdatabehandler gjør hele eller deler av behandlingen av personopplysninger på vegne av en databehandler og ikke på vegne av en behandlingsansvarlig.

Eksempel 1: Dersom virksomhet A lagrer personopplysninger på vegne av virksomhet B, er virksomhet B å anse som en databehandler.

Eksempel 2: Virksomhet A er databehandler for virksomhet B. Virksomhet A inngår avtale med virksomhet C for å utføre hele eller deler av behandlingen som virksomhet A gjør i kraft av å være databehandler. Virksomhet C er å anse som underdatabehandler.

Underdatabehandlere

Basert på eksplisitt skriftlig godkjenning fra behandlingsansvarlig kan databehandleren benytte seg av en underdatabehandler til å gjøre hele eller deler av behandlingen av personopplysninger.

Eksempel: Virksomhet B er databehandler for virksomhet A. I henhold til databehandleravtalen mellom virksomhet A og B skal virksomhet B blant annet lagre personopplysninger på vegne av virksomhet A. Virksomhet B ønsker å benytte virksomhet C til å lagre personopplysningene. Virksomhet C er å anse som en underdatabehandler.

Databehandleravtaler

Dersom den behandlingsansvarlige benytter seg av en databehandler, har den behandlingsansvarlige en plikt til å inngå en databehandleravtale med databehandleren. Den skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysningene. Avtalen må være et rettslig bindende dokument.

Også hvis databehandleren benytter seg av en databehandler til å gjøre hele eller deler av behandlingen av personopplysninger, må det inngås en databehandleravtale mellom databehandleren og underdatabehandleren.

Eksempel 1: Virksomhet A benytter seg av virksomhet B som databehandler. Virksomhet A må inngå databehandleravtale med virksomhet B.

Eksempel 2: Virksomhet A er databehandler for virksomhet B. Virksomhet B benytter seg av virksomhet C til å gjøre hele eller deler av behandlingen av personopplysninger. Både virksomhet A og B og virksomhet B og C må inngå databehandleravtaler.

Felles behandlingsansvar

For definisjon av felles behandlingsansvar, se begrepsliste.

Ved felles behandlingsansvar kan begge behandlingsansvarlige inngå avtale med databehandlere. Hvis så tilfellet må avtalen om felles behandlingsansvar si noe om inngåelse av avtale med aktuelle databehandlere. En slik avtale skal tilfredsstille alle krav etter GDPR art. 28 og ellers videreføre alle plikter som er nødvendige, for at behandlingsansvarlige som benytter seg av databehandler kan overholde sine forpliktelser overfor den annen part.

Hver av partene skal kontrollere at egne databehandlere overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underdatabehandlere er kjent med sine forpliktelser og oppfyller disse.

Endringer i bruk av databehandlere skal forhåndsgodkjennes av den annen part før nye avtaler inngås. Kopi av inngåtte databehandleravtaler skal fremlegges for den annen part på forespørsel.

Eksempel: Virksomhet A og B inngår avtale om felles behandlingsansvar. Virksomhet A inngår avtale med en databehandler. Avtalen om felles behandlingsansvar må si noe om at det inngås avtale med eventuelle databehandlere.

Samarbeidsavtale, kravspesifikasjon e.l.

Virksomheten må alltid kontrollere hvordan databehandleravtalen står i forhold til samarbeidsavtalen. Ofte vil en samarbeidsavtale anses som hovedavtalen mellom behandlingsansvarlig og databehandler. Databehandleravtalen vil da være et tillegg til samarbeidsavtalen, men databehandleravtalen kan også inngå som en del av samarbeidsavtalen. Både når databehandleravtalen er et tillegg til samarbeidsavtalen og når databehandleravtalen er en del av samarbeidsavtalen, må man påse at det ikke er motstrid mellom samarbeidsavtalen og databehandleravtalen. I tillegg må man påse at alle krav til databehandleravtale i henhold til GDPR er oppfylt.

Allerede ved anskaffelsen av leverandør (databehandler) må behandlingsansvarlig i kravspesifikasjonen stille krav til bla. personvern og informasjonssikkerhet.

Eksempel: Virksomhet A skal anskaffe en leverandør av skytjenester for lagring av personopplysninger. Allerede ved utforming av kravspesifikasjon stiller behandlingsansvarlig krav til innebygd personvern.

# Til kapitel 8 PLM og DPIA (Risiko og tiltak)

I malen skal uønskede hendelser og restrisiko fra ROSen fylles inn. Det er viktig å merke seg at en ROS kan oppdateres flere ganger, men de uønskede hendelsene og restrisiko som overføres til DPIA må ha en konkret dato som er tidspunkt for gjennomføring av DPIA.

## Risikoanalyse

I en risikoanalyse skal virksomhetene vurdere og avklare aktuelle personvernkonsekvenser for den registrerte dersom ulike typer uønskede hendelse inntreffer, med bakgrunn i hvor inngripende behandlingen av personopplysningene er. En uønsket hendelse i dette tilfellet er når behandlingen av personopplysninger kan medføre forringelse av den registrertes rettigheter og friheter. Virksomhetene skal ta utgangspunktet fra den registrerte side, da verdiene man ønsker å beskytte er den registrertes rettigheter og friheter. For eksempel må man vurdere om behandlingen medfører en økt fare for å krenke rettighetene til den registrerte. Det er med andre ord den registrertes perspektiv som er viktig. En slik vurdering vil dermed være forskjellig fra hvordan man foretar en risikoanalyse på informasjonssikkerhet, da fokuset vil være ut fra virksomhetens perspektiv.

Også når det gjelder tiltakene som foreslås iverksatt, må virksomhetene fokusere på hvilke endringer man kan gjøre på behandlingen og/eller hvordan rettighetene ivaretas, i stedet for å tenke på hvilke sikkerhetstiltak man kan iverksette da disse nødvendigvis ikke tar ned risikoen for den registrertes rettigheter og friheter. Det er videre viktig at de skisserte tiltakene faktisk gjennomføres, og hvis dette ikke gjøres vil ikke det oppgitte risikobildet være reelt og DPIA’en må oppdateres og godkjennes på nytt av ledelsen til virksomheten. Dette gjelder også ved risikoanalyse på personopplysningssikkerheten.

Malen for DPIA risikoanalyse er inndelt etter de ulike personvernprinsippene, den registrertes rettigheter og den registrertes friheter. Merk at prinsippet om konfidensialitet og integritet ikke er med i denne risikoanalysen. Dette fordi disse prinsippene tas ved risikovurderingen knyttet til personopplysningssikkerhet (og informasjonssikkerhet).

Eksempler på personvernhendelser og risikoanalyse ligger vedlagt. I vedlegget er det satt opp noen mulige hendelser for en tenkt virksomhet. Dette er kun et eksempel og hver virksomhet må vurdere konkret hva som er relevante for sitt tilfelle og hvilke scenarioer som er relevante å ta i betraktning. Ved mer komplekse vurderinger kan det være hensiktsmessig å gjøre vurderingene i flere omganger, knyttet opp til hver del.

Det er anledning til å legge til og tilpasse scenarioene etter behov, slik at det treffer virksomhetens planlagte behandlingsaktivitet på best mulig måte.

## Risikomatrise

Risikomatrisen skal hjelpe virksomhetene å oppsummere og beskrive risikoen knyttet til de to dimensjonene, konsekvens og sannsynlighet. Sannsynlighet er muligheten for at risikoen skal inntreffe. Konsekvens er hvor alvorlig risikoen er for den registrertes rettigheter og friheter.

For å vurdere personvernkonsekvenser, tas det utgangspunkt i personvernprinsippene og hvordan disse er ivaretatt for å sikre de registrertes rettigheter og friheter. Dette er lovfestede krav etter personvernregelverket og en gjennomgang av kravene vil gi en god indikator på hvordan en virksomhet ligger an med ivaretakelsen av kravene i regelverket og hvilke prinsipper som medfører de største utfordringene for den behandlingsaktiviteten som vurderes. Ved vurderingen er det viktig at virksomheten tar hensyn til at ulike faktorer kan medføre at konsekvensnivået endres.

Hendelsene presenteres i en matrise som illustrerer risikonivået. Ved å plassere hendelsene i en felles matrise vil det blir enklere å sammenligne risiko for virksomheten. Under beskrives de kombinasjoner av nivå på konsekvens og sannsynlighet som skal brukes for å fastsette risikonivå:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Sannsynlighet*** | **Svært sannsynlig** |  |  |  |  |  |
| **Sannsynlig** |  |  |  |  |  |
| **Moderat** |  |  |  |  |  |
| **Lite sannsynlig**  |  |  |  |  |  |
| **Svært lite sannsynlig** |  |  |  |  |  |
| **RISIKO** | **Ubetydelig**  | **Lav**  | **Moderat** | **Alvorlig** | **Svært alvorlig**  |
| ***Konsekvens*** |

**Sannsynlighetsnivå**

Sannsynlighet beskriver hvor ofte og hvor lett en hendelse kan forventes å inntreffe i fremtiden. Sannsynlighet kan basere seg på flere faktorer, herunder hvor reell fare det er for at hendelsen inntreffer, hvilke tiltak er allerede implementert for å begrense sannsynligheten mv. For behandlingsaktiviteter som skal pågå i over ett år er det viktig at virksomheten foretar vurderinger basert på årlig tilnærming.

|  |  |  |
| --- | --- | --- |
| **Nivå** | **Beskrivelse**  | **Veiledning**  |
| **1** | **Svært liten sannsynlighet** | Mindre enn 5% sannsynlig at de vil inntreffe.Hendelsen kan oppstå helt spesielle omstendigheter. |
| **2** | **Det er lite sannsynlig at de vil inntreffe**  | 5- 10% sannsynlig at de vil inntreffe.Hendelsen kan oppstå under sjeldne omstendigheter.  |
| **3** | **Det er moderat sannsynlig at de vil inntreffe** | 10-30% sannsynlig at de vil inntreffe.Hendelsen kan oppstå under noen omstendigheter.  |
| **4** | **Det er sannsynlig at de vil inntreffe** | 30-70% sannsynlig at de vil inntreffe. Hendelsen kan oppstå under flere omstendigheter.  |
| **5** | **Det er nesten sikkert/svært sannsynlig at de vil inntreffe** | Over 70% sannsynlig at de vil inntreffe. Hendelsen kan oppstå under de fleste omstendigheter. |

**Konsekvensnivå**

Konsekvensen av at rettighetene og frihetene ikke blir innfridd kan være både være fysisk, materiell og ikke-materiell skade. Det er viktig at virksomhetene er bevisste på at konsekvensen behandlingen har for de registrerte ikke er avhengig av at det skjer en hendelse, men at konsekvensen også kan inntreffe gjennom selve behandlingen i seg selv.

Dette kan for eksempel være:

* + Behandlingen kan gi økonomisk tap for den registrerte
	+ Behandlingen kan påvirke omdømmet til den registrerte
	+ Behandlingen kan medføre mulighet for stigmatisering
	+ Behandlingen kan være diskriminerende
	+ Behandlingen kan medføre forskjellsbehandling blant søkere hos NAV
	+ Behandlingen kan føre til identitetstyveri eller bedrageri på grunn av manglende sikkerhet
	+ Behandlingen kan være en direkte krenkelse av privatlivets fred
	+ Behandlingen kan medføre inngrep i ytringsfriheten eller tankefriheten hos den registrerte
	+ Behandlingen kan begrense handlefriheten til den registrerte
	+ Behandlingen kan svekke selvtilliten til den registrerte
	+ Behandlingen kan medføre at den enkelte ikke får oppfylt sine personvernrettigheter:
		- Rett til innsyn
		- Rett til informasjon
		- Rett til å protestere mot automatisk behandling
		- Rett til innsigelse
		- Rett til korrigering
		- Rett til å bli glemt (sletting)
		- Rett til dataportabilitet
		- Rett til begrenset behandling

Merk at forskjellen på når den aktuelle konsekvensen for den registrertes personvern er alvorlig og svært alvorlig er at sistnevnte vil inntreffe når virksomhetene ikke klarer å iverksette tiltak som tar ned risikoen.

Tabellen under beskriver nærmere konsekvensnivåene.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nivå** | **Beskrivelse**  | **Konsekvenser for etterlevelse av regelverket (GDPR)** | **Konsekvens for den registrerte** | **Konsekvens for virksomhet (for etterlevelse av lov, forskrift og avtaler)** |
| **1** | **Den aktuelle konsekvensen for den registrerte er ubetydelig**  | * Den registrertes rettigheter påvirkes ikke.
* Den registrertes friheter ikke.
* De grunnleggende prinsippene blir ivaretatt
 | * Hendelsen fører ikke til noen helsemessige konsekvenser for den registrerte
* Hendelsen fører ikke til økonomisk tap for den registrerte
* Hendelsen vil ikke påvirke den registrertes omdømme
* Hendelsen vil ikke påvirke den registrertes rettigheter.
* Hendelsen vil ikke påvirke den registrertes friheter.
* Den registrertes tillit til Oslo kommune vil ikke påvirkes.
 | * Hendelsen påvirker ikke etterlevelse.
 |
| **2** | **Den aktuelle konsekvensen for den registrertes personvern er lav**  | * Den registrertes rettigheter påvirkes i mindre grad
* Den registrertes friheter påvirkes i mindre grad
* De grunnleggende prinsippene blir i hovedsak ivaretatt
 | * Hendelsen kan føre til midlertidige eller mindre alvorlige fysiske og/eller psykiske helsemessige konsekvenser for den registrerte.
* Hendelsen kan føre til forbigående økonomisk tap for den registrerte.
* Hendelsen kan føre til midlertidig eller begrenset tap av den registrertes omdømme.
* Hendelsen kan føre til at den registrertes (rett til personvern) rettigheter ikke er tilstrekkelig ivaretatt i en svært kort periode.
* Hendelsen kan føre til at den registrertes (rett til personvern) friheter ikke er tilstrekkelig ivaretatt i en svært kort periode.
* Den registrertes tillit til Oslo kommune utfordres midlertidig.
 | * Hendelsen kan medføre brudd på intern instruks eller reglement, uten at dette medfører brudd på lov, forskrift eller annet regelverk.
 |
| **3** | **Den aktuelle konsekvensen for den registrertes personvern er moderat** | * Den registrertes rettigheter påvirkes i noe grad
* Den registrertes friheter påvirkes i noe grad
* De grunnleggende prinsippene blir ivaretatt i noe grad
 | * Hendelsen kan føre til midlertidige eller noe mer alvorlige fysiske og/eller psykiske helsemessige konsekvenser for den registrerte.
* Hendelsen kan føre til økonomisk tap av noe varighet for den registrerte.
* Hendelsen kan føre til midlertidige eller noe mer alvorlige tap av den registrertes omdømme.
* Hendelsen kan føre til at den registrertes (rett til personvern) rettigheter ikke er tilstrekkelig ivaretatt i en svært kort periode.
* Hendelsen kan føre til at den registrertes (rett til personvern) friheter ikke er tilstrekkelig ivaretatt i en svært kort periode.
* Den registrertes tillit til Oslo kommune utfordres
 | * Hendelsen kan medføre eller bidra til brudd på lov, forskrift eller annet regelverk.
 |
| **4** | **Den aktuelle konsekvensen for den registrertes personvern er alvorlig for den registrertes personvern** | * Den registrertes rettigheter påvirkes i stor grad
* Den registrertes friheter påvirkes i stor grad
* De grunnleggende prinsippene blir i stor grad ikke ivaretatt
 | * Hendelsen kan føre til varige eller alvorlige fysiske og/eller psykiske helsemessige konsekvenser for den registrerte.
* Hendelsen kan føre økonomisk tap av betydelig varlighet for den registrerte.
* Hendelsen kan føre til varig eller alvorlig tap av den registrertes omdømme.
* Hendelsen kan føre til at den registrertes (rett til personvern) rettigheter krenkes på en alvorlig måte
* Hendelsen kan føre til at den registrertes andre rettigheter krenkes på en alvorlig måte
* Hendelsen kan føre til at friheter krenkes på en alvorlig måte.
* Den registrerte taper tilliten til Oslo kommune.
 | * Hendelsen kan medføre eller bidra til alvorlig brudd på lov, forskrift eller annet regelverk.
 |
| **5** | **Den aktuelle konsekvensen for den registrertes personvern er svært alvorlig**  | * Den registrertes rettigheter blir ikke ivaretatt
* Den registrertes friheter blir ikke ivaretatt
* De grunnleggende prinsippene blir ikke ivaretatt
 | * Hendelsen kan føre til tap av liv (for den registrerte).
* Hendelsen kan føre til varige og alvorlige fysiske og/eller helsemessige konsekvenser for den registrerte.
* Hendelsen kan føre til varig og betydelig økonomisk tap for den registrerte.
* Hendelsen kan føre til varig og alvorlig tap av den registrertes omdømme.
* Hendelsen kan føre til at den registrertes rettigheter (rett til personvern) krenkes på en svært alvorlig måte.
* Hendelsen kan føre til at den registrertes andre rettigheter krenkes på en svært alvorlig måte.
* Hendelsen kan føre til at friheter krenkes på en svært alvorlig måte.
* Den registrerte og samfunnet taper tilliten til Oslo kommune.
 | * Hendelsen medfører alvorlig brudd på lov, forskrift eller annet regelverk
 |

1. Oversikt over godkjente tredjeland finner man her: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/> [↑](#footnote-ref-1)
2. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/sarlig-om-standard-personvernbestemmelser-som-overforingsgrunnlag/> [↑](#footnote-ref-2)
3. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/sarlig-om-bcr-som-overforingsgrunnlag/> [↑](#footnote-ref-3)
4. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/nodvendig-for-a-ivareta-legitime-interesser---interesseavveiing/> [↑](#footnote-ref-4)
5. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/> [↑](#footnote-ref-5)
6. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/> [↑](#footnote-ref-6)
7. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/dataminimering/> [↑](#footnote-ref-7)
8. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/dataminimering/> [↑](#footnote-ref-8)
9. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/lagringsbegrensning/> [↑](#footnote-ref-9)
10. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/integritet-og-konfidensialitet/> [↑](#footnote-ref-10)
11. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/ansvarlighet/> [↑](#footnote-ref-11)
12. <https://felles.intranett.oslo.kommune.no/getfile.php/132446412/%5BFI%5D%20Felles%20intranett/05-Informasjonssikkerhet/Personvern/Veileder%20innsyn%20v.%201.0_.pdf> [↑](#footnote-ref-12)