



Oslo

Byrådsavdeling for finans

Veileder om behandlingsgrunnlag

En veileder om hvordan vurdere
riktig behandlingsgrunnlag ved
behandling av personopplysninger.



Om veilederen

Gjennom personopplysningsloven er EUs personvernforordning (GDPR) gjort til en del av norsk rett.

I henhold til GDPR artikkel 6 nr.1 kreves det et behandlingsgrunnlag for at behandling av personopplysninger skal være lovlig. Hvis personopplysningene allerede er samlet inn for et formål og skal viderebehandles, krever GDPR art.6 nr.4 at det er forenlighet mellom opprinnelig formål og nytt formål for behandlingen.

Veilederen vil gi leseren hjelp til hva som skal vurderes for å finne lovlig behandlingsgrunnlag ved førstegangsbehandling av personopplysninger og hvordan særlige kategorier (sensitive) personopplysninger kan behandles lovlig. Veilederen vil også være til hjelp når forenligheten mellom det opprinnelige formålet og det nye formålet skal vurderes ved viderebehandling av personopplysninger.

Formål

Formålet med veilederen er å bidra til å sikre etterlevelse av lover, regelverk og kommunens styrende dokumenter ved å gi ansatte og ledere i Oslo kommune konkret veiledning for vurdering av behandlingsgrunnlag. Dette dokumentet gir informasjon om hvilke problemstillinger som må vurderes i saksbehandlingsprosessen.

Veilederen skal bidra til å ivareta at all behandling av personopplysninger har et lovlig behandlingsgrunnlag og at viderebehandling av personopplysninger er forenlig med opprinnelig formål.

Virksomheter i Oslo kommune vil ha ulike behov og ulikt utgangspunkt for å vurdere behandlingsgrunnlag. Veilederen vil derfor ikke besvare konkrete problemstillinger i hver enkelt sak siden omstendighetene vil variere.

Målgruppe

Dokumentet skal gi veiledning til ansatte og ledere i Oslo Kommune som er involvert i vurdering av behandlingsgrunnlag, samt ansatte med definerte oppgaver innen personvern. Dette omfatter f.eks. personvernkoordinatorer, systemeiere, systemforvaltere, andre ressurser innen personvern mv.

Anvendelsesområdet

Veilederen kan brukes når det planlegges å starte en behandling av personopplysninger. Videre kan veilederen brukes når virksomheten planlegger å viderebehandle personopplysninger som allerede er innsamlet for et annet formål.

Innhold

1	Sentrale begreper ved vurdering av behandlingsgrunnlag	4
1.1	Personopplysninger.....	4
1.2	Særlige kategorier personopplysninger	4
1.3	Behandling av personopplysninger.....	4
1.4	Formål	4
1.5	Behandlingsgrunnlag.....	5
1.6	Supplerende rettsgrunnlag.....	5
1.7	Viderebehandling av personopplysninger	5
2	Hvorfor må man ha behandlingsgrunnlag?	5
3	Førstegangsbehandling av personopplysninger	6
3.1	Hva bør man tenke på før vurdering av behandlingsgrunnlag?	7
3.2	Behandlingsgrunnlag etter GDPR art. 6	8
3.3	Behandling av særlige kategorier personopplysninger etter GDPR art.9	10
3.4	Nærmere om samtykke	11
3.5	Nærmere om berettiget interesse.....	12
4	Viderebehandling av personopplysninger.....	12
4.1	Hvordan gå frem ved viderebehandling av personopplysninger?	12
4.2	Forenlighetstest	13
5	Oppsummering	15

1 Sentrale begreper ved vurdering av behandlingsgrunnlag

1.1 Personopplysninger

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f. eks et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

1.2 Særlige kategorier personopplysninger

Særlige kategorier personopplysninger er personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Særlige kategorier personopplysninger ble tidligere kalt sensitive personopplysninger.

Særlige kategorier personopplysninger krever særlig beskyttelse, og det er derfor strengere krav til behandling av denne typen personopplysninger. Det vil f. eks kreves mer av hvilke tiltak som gjennomføres for å beskytte særlige kategorier personopplysninger.

1.3 Behandling av personopplysninger

Behandling av personopplysninger er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f. eks innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensnig, sletting eller tilintetgjøring.

Dette betyr kort fortalt alle handlinger som kan gjøres med personopplysningene, enten det er manuelt eller digitalt.

1.4 Formål

Hva skal opplysningene brukes til? Formålet med behandlingen av opplysningene er hensikten eller planen med innsamlingen av opplysningene. GDPR krever at personopplysninger bare kan samles inn til spesifikke, uttrykkelig angitte og berettigede formål og at personopplysningene ikke kan viderebehandles på en måte som er uforenlig med dette formålet.

Formålet må bestemmes før behandlingen startes.

1.5 Behandlingsgrunnlag

All behandling av personopplysninger må ha et rettslig grunnlag, dette kalles behandlingsgrunnlag og er kjernen i lovlighetsprinsippet i GDPR. Både behandlingsgrunnlag, rettsgrunnlag og hjemmel for behandlingen blir brukt for å beskrive dette kravet. Det finnes flere behandlingsgrunnlag, se mer i punkt 3.2 nedenfor. Eksempler på behandlingsgrunnlag kan være samtykke fra den det skal behandles opplysninger om eller at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse (f. eks lovpålagte oppgaver i kommunen).

1.6 Supplerende rettsgrunnlag

Supplerende rettsgrunnlag er når GDPR krever at noen av behandlingsgrunnlagene må ha et ekstra rettsgrunnlag i den nasjonale lovgivningen.

Dette gjelder når behandlingsgrunnlaget er nødvendig for å oppfylle en rettslig forpliktelse eller når det er en behandling som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.

1.7 Viderebehandling av personopplysninger

Viderebehandling eller gjenbruk av personopplysninger betyr at opplysningene allerede er samlet inn til et formål (opprinnelig formål), og at det planlegges å behandle personopplysningene til et nytt formål.

Hvis en viderebehandling skal være lovlig, må det nye formålet være forenlig med det opprinnelige formålet opplysningene ble samlet inn for.

2 Hvorfor må man ha behandlingsgrunnlag?

Det er flere grunner til at det er viktig å få på plass behandlingsgrunnlag før behandlingen starter.

- ▶ **Lovkrav:** Det viktigste er at behandlingen ikke er lovlig uten behandlingsgrunnlag. Dette er et krav i GDPR for å være i tråd med lovlighetsprinsippet, som krever at all behandling skal ha et rettslig grunnlag.
- ▶ **Dokumentasjonsplikt:** Som behandlingsansvarlig har man en plikt til å ha dokumentasjon for at behandlingen er lovlig, det betyr at vurderingen av behandlingsgrunnlag bør dokumenteres på en god måte og den må være tilgjengelig på forespørsel fra f. eks for Datatilsynet eller ved revisjon i virksomheten.
- ▶ **Informasjonsplikt:** Behandlingsgrunnlag er også en forutsetning for å gi riktig informasjon til den registrerte i personvernerklæringen eller når det kommer forespørsler om innsyn eller informasjon fra den registrerte. I tillegg er informasjon om behandlingsgrunnlag

nødvendig for å kunne fylle ut behandlingsoversikt/protokoll som behandlingsansvarlige har en plikt til å ha.

- ▶ **Formålsbegrensning:** Et annet viktig prinsipp når det gjelder behandlingsgrunnlag er formålsbegrensningsprinsippet. Formålsbegrensningsprinsippet er et grunnleggende personvernprinsipp som sier at personopplysninger bare kan samles inn for «spesifikke, uttrykkelig angitte og berettigede formål. Formålet har derfor stor betydning for å finne riktig behandlingsgrunnlag.

3 Førstegangsbehandling av personopplysninger

Dette kapittelet gir veiledning omen ny behandling av personopplysninger, dvs. når personopplysningene ikke allerede er innsamlet for et annet formål. Hvis personopplysningene opprinnelig er samlet inn for et annet formål, gå til viderebehandling i kapittel 4 nedenfor.

Som nevnt over, må all behandling av personopplysninger ha et rettslig grunnlag for å oppfylle lovlighetsprinsippet. Det må derfor finnes et behandlingsgrunnlag for den planlagte behandlingen i GDPR art.6 nr.1. Det er flere alternative behandlingsgrunnlag, og vilkårene for minst ett behandlingsgrunnlag må være oppfylt. Dersom det er snakk om flere behandlinger og formål, kan det være snakk om flere behandlingsgrunnlag. Se nærmere om hvilke behandlingsgrunnlag som finnes i punkt 3.2 nedenfor. Hvis det skal behandles særlige kategorier personopplysninger må det i tillegg til behandlingsgrunnlag også finnes et unntak i GDPR art.9 nr.2, se mer nedenfor i punkt 3.3 om dette.

Husk at behandlingsgrunnlaget må dekke alle behandlingsaktiviteter som er planlagt for å oppnå formålet. Behandlingsgrunnlagene er likestilte, dvs. at ingen av behandlingsgrunnlagene er rangert høyere enn de andre.

Hvis man skal behandle personopplysninger er det en forutsetning at behandlingen er nødvendig for å oppnå formålet (gjelder ikke samtykke). Hvis det er mulig å oppnå formålet uten å behandle personopplysningene, vil ikke kravet til at behandlingen er nødvendig være oppfylt og man kan derfor ikke behandle personopplysningene

Det å finne riktig behandlingsgrunnlag er en grunnleggende vurdering når man skal behandles personopplysninger, men det betyr ikke at denne vurderingen alene er tilstrekkelig som vurdering av personvernet ved behandlingen. Det er flere krav i regelverket til andre vurderinger som må gjøres. Hvis behandlingen f. eks innebærer en høy risiko for den registrertes rettigheter og friheter, krever GDPR at det gjennomføres en personvernkonsekvensvurdering (DPIA). Hvis behandlingen ikke innebærer en høy risiko må det fortsatt gjøres grunnleggende personvern vurderinger, f. eks hvordan personvernprinsippene i GDPR og kravene til den registrertes rettigheter skal ivaretas.

3.1 Hva bør man tenke på før vurdering av behandlingsgrunnlag?

Det er flere momenter virksomheten bør ta stilling til før vurderingen av behandlingsgrunnlag starter, blant annet:

- ▶ **Formål:** En tydelig formålsbeskrivelse bør være på plass før man skal vurdere behandlingsgrunnlaget. Formålet er en forutsetning for å vurdere om behandlingen er lovlig og hva som er riktig behandlingsgrunnlag. Når formålet skal beskrives er det viktig at det dekker det man planlegger å bruke opplysningene til, samtidig bør formålet være detaljert og tydelig nok til å dekke kravet til at formålet skal være spesifikt og uttrykkelig angitt. Formålet må også være berettiget, dvs. at det må være rimelige grunner til at virksomheten skal behandle personopplysningene.
- ▶ **Type personopplysninger:** Hvilke personopplysninger man planlegger å behandle, kan ha betydning for å finne riktig behandlingsgrunnlag. Husk at det er et krav å behandle så få personopplysninger som mulig for å oppnå formålet (dataminimeringsprinsippet). Videre er det nødvendig å vite hvilke personopplysninger for å avklare om det er snakk om særlige kategorier personopplysninger som i tillegg til behandlingsgrunnlag krever unntak i GDPR art.9. F. eks hvis det kun er snakk om å behandle navn, e-postadresse og mobilnummer uten at det skal skje sammenstilling med annen informasjon, vil det ikke være nødvendig å se hen til unntakene i GDPR art.9, men kun finne behandlingsgrunnlag i GDPR art.6.
- ▶ **Hvem som er behandlingsansvarlig:** Hvem som er behandlingsansvarlig har betydning ved vurderingen av behandlingsgrunnlag. Et av behandlingsgrunnlagene (berettiget interesse) kan ikke brukes som behandlingsgrunnlag når behandlingen utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver. Husk at behandlingsgrunnlaget likevel kan brukes når den aktuelle virksomheten utøver andre oppgaver som *ikke* er offentlig myndighet, f. eks test av løsningen eller lignende. I Oslo kommune vil en del av behandlingen ikke være offentlig myndighet, f. eks når Oslo kommune opptre som arbeidsgiver og behandler personopplysninger i den sammenhengen. I slike tilfeller kan berettiget interesse fortsatt være et aktuelt behandlingsgrunnlag.
- ▶ **Hvilke behandlinger av personopplysninger:** Det bør være avklart hvilke behandlinger av personopplysningene som planlegges, fordi det er et krav at behandlingen skal være *nødvendig* for å oppnå formålet. Eksempler på behandling kan være innsamling, lagring, sammenstilling osv.
- ▶ **Kilde til personopplysninger:** Hvor personopplysningene hentes fra er av betydning for behandlingsgrunnlaget. Hvis personopplysningene skal hentes direkte fra den personopplysningene handler om, vil det ofte være snakk om samtykke som behandlingsgrunnlag., Hvis personopplysningene hentes fra andre kilder (f. eks et register), må det sikres at det er lov til å hente personopplysninger fra kilden til det aktuelle formålet og at virksomhetene har behandlingsgrunnlag.

3.2 Behandlingsgrunnlag etter GDPR art. 6

Nedenfor gis kort informasjon om de enkelte behandlingsgrunnlagene i GDPR art.6 nr.1. Det finnes mer informasjon på Datatilsynets hjemmesider.¹

a) Samtykke

Et samtykke er en viljeserklæring fra den registrerte som gis frivillig. Det stilles flere krav til hva som er et gyldig samtykke og når det ikke kan brukes som behandlingsgrunnlag, se nærmere om dette i punkt 3.4 om samtykke nedenfor.

b) Avtale

Husk at dette behandlingsgrunnlaget ikke kan brukes for behandlinger av personopplysninger som ikke er nødvendige for å oppfylle avtalen. Behandlingsansvarlig kan f. eks ikke lage ensidige vilkår med «liten skrift» for behandlinger som er ønskelige men ikke nødvendige, f. eks behandlinger for markedsføringsformål.

c) Rettslig forpliktelse

Husk at den rettslige forpliktelsen må være en plikt for den behandlingsansvarlige. Dette behandlingsgrunnlaget krever *supplerende rettsgrunnlag*, f. eks lovpålagte oppgaver for kommunen.

d) Vitale interesser

Vitale interesser er et behandlingsgrunnlag som er svært snevert, og som kun kan brukes når det er snakk om liv og død, eller når det er fare for helsen. Det kan være snakk om den vitale interessen til den personopplysningene handler om eller noen andre. Behandlingsgrunnlaget kan som sagt bare brukes helt unntaksvis f. eks i forbindelse med livreddende helsehjelp og det ikke er mulig å finne et annet behandlingsgrunnlag pga. tid eller når personen ikke er i stand til å samtykke. Det kan f. eks være snakk om å dele personopplysninger om pasienten med en lege som er ekspert på et medisinsk fagfelt, men som ikke behandler pasienten.

e) Allmenhetens interesse eller utøvelse av offentlig myndighet

En virksomhet kan behandle personopplysninger hvis det er nødvendig for å utføre en oppgave i allmenhetens interesse eller hvis behandlingen er nødvendig for å utøve offentlig myndighet den behandlingsansvarlige er pålagt. Dette behandlingsgrunnlaget er i størst grad aktuelt for offentlige myndigheters behandling av personopplysninger, men kan også være aktuelt der private virksomheter er tillagt offentlig myndighet eller skal utføre oppgaver i allmenhetens interesse.

¹ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/>

Det kreves ikke for dette behandlingsgrunnlaget at virksomheten er pålagt en rettslig forpliktelse (se ovenfor i punkt c), men husk at det kreves et supplerende rettsgrunnlag i nasjonal lovgivning i tillegg.

f) Berettiget interesse

Virksomheten kan behandle personopplysninger for å ivareta en berettiget interesse. Den berettigede interessen må være lovlig, den må defineres på forhånd, den må være reell og saklig begrunnet i virksomheten. Behandlingen av personopplysningen må være nødvendig for den berettigede interessen. Dette betyr at hvis formålet kan oppnås på en annen måte som er mindre inngripende for personvernet, så kan ikke behandlingen gjennomføres.

For dette behandlingsgrunnlaget er det et krav at virksomheten foretar en interesseavveining mellom den berettigede interessen de har i å behandle personopplysningene og personvernulempene for de berørte. Se nærmere om interesseavveining i punkt 3.5 nedenfor.

Husk at dette behandlingsgrunnlaget ikke kan brukes på behandlinger som utføres av offentlige myndigheter som ledd i deres oppgave. Berettiget interesse kan likevel være aktuelt der offentlige myndigheter utfører oppgaver som ikke er offentlig myndighet, f. eks i kraft av å være arbeidsgiver.

Hvis behandlingsgrunnlaget er en rettslig forpliktelse eller en oppgave i allmennhetens interesse/utøvelse av offentlig myndighet, er det krav om supplerende rettsgrunnlag. Det betyr at virksomheten må finne hjemmel i nasjonal lovgivning i tillegg til behandlingsgrunnlaget. Denne hjemmelen må dekke den behandlingen av personopplysninger som planlegges. Det trenger ikke stå konkret i bestemmelsen at det skal behandles personopplysninger, men behandlingen av personopplysninger må være nødvendig for å kunne oppfylle den rettslige forpliktelsen som ligger i bestemmelsen.

Hvis kommunen er pålagt en oppgave ved lov vil f. eks rettslig forpliktelse være behandlingsgrunnlaget etter GDPR art.6 nr.1 bokstav c), mens bestemmelsen i loven der oppgaven er pålagt er det supplerende rettsgrunnlaget. Se som eksempel i helse- og omsorgstjenesteloven § 3-7 der kommunen pålegges å skaffe boliger til personer som ikke selv kan ivareta sine interesser på boligmarkedet. Bestemmelsen vil kunne gi behandlingsgrunnlag for å behandle nødvendige opplysninger om enkeltpersoner for at kommunen skal kunne yte denne tjenesten (f. eks navn, kontaktopplysninger, informasjon om boligbehov, behov for oppfølging mv.).

3.3 Behandling av særlige kategorier personopplysninger etter GDPR art.9

Behandling av særlige kategorier personopplysninger er i utgangspunktet forbudt, men det finnes flere unntak som gir behandlingsgrunnlag i GDPR art.9 nr.2. Flere av unntakene, som f. eks samtykke og vitale interesser, overlapper med behandlingsgrunnlagene etter GDPR art.6 nr.1, i så fall gjelder beskrivelsene etter art.6 nr.1 også her.

Hvis behandlingen omfatter særlige kategorier personopplysninger, betyr det at virksomheten først må finne behandlingsgrunnlag i GDPR art.6 nr.1, så finne et unntak i GDPR art.9 nr.2 som dekker behandlingen. Etter dette må virksomheten finne supplerende rettsgrunnlag hvis det er snakk om å bruke rettslig forpliktelse (GDPR art.6 nr.1 bokstav c) eller oppgaver i allmenhetens interesse/offentlig myndighet som behandlingsgrunnlag (GDPR art.6 nr.1 bokstav e).

Et eksempel på bruk av supplerende rettsgrunnlag der rettslig forpliktelse er behandlingsgrunnlaget, er hvis man skal samle inn helseopplysninger i forbindelse med pasientbehandling. Behandlingsgrunnlaget i GDPR art.6 vil være bokstav c) «rettslig forpliktelse». Deretter vil unntaket og behandlingsgrunnlag etter GDPR art.9 nr.2 være bokstav h) «yting av helse- eller sosialtjenester». Det supplerende rettsgrunnlaget i nasjonal lovgivning vil kunne være pasientjournalloven §8 (som gir en virksomhet som yter helsehjelp plikt til å ha journal), jf. helsepersonelloven § 39 (helsepersonells dokumentasjonsplikt, dvs. plikten til å føre journal).

Nedenfor gis en kort oversikt over unntakene for behandling av særlige kategorier av personopplysninger i GDPR art.9 nr.2. Det finnes mer informasjon på Datatilsynets hjemmesider.²

- a) Den registrerte har gitt et uttrykkelig samtykke
- b) Behandlingen er nødvendig for at den behandlingsansvarlige eller registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett
- c) Behandlingen er nødvendig for å verne vitale interesser
- d) Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art
- e) Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort
- f) Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet
- g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser
- h) Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk,

² <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger-sensitive-personopplysninger-og-unntak/>

yting av helse- eller omsorgstjenester, behandling eller forvaltning av helse- eller sosialtjenester og –systemer (husk det særlige krav om lovbestemt taushetsplikt for dette unntaket)

- i) Behandlingen er nødvendig av allmenne folkehelsehensyn eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr
- j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål

Husk at det er mange forbehold ved bruk av disse unntakene, og at man må sette seg godt inn i hver enkelt bestemmelse før den kan brukes. Flere av bestemmelsene (GDPR art.9 nr.2 bokstavene b, g, h, i og j) krever i tillegg at det finnes en hjemmel i nasjonal lovgivning for at unntaket skal kunne brukes.

I tillegg til unntakene i GDPR art.9 nr.2, finnes det noen egne unntak i den norske personopplysningsloven §§ 6-9 for behandling av særlige kategorier av personopplysninger:

- i arbeidsforhold der det er nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter
- etter særlig tillatelse fra Datatilsynet
- for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål

3.4 Nærmere om samtykke

For at et samtykke skal være gyldig, må det være:

- frivillig
- spesifikt
- informert
- utvetydig

Samtykke skal gis i en forståelig og lett tilgjengelig form og på et klart og enkelt språk. I tillegg skal samtykket gis ved en aktiv handling og det skal være like lett å trekke samtykket som å gi. Samtykket være dokumenterbart.

Datatilsynet gir nærmere veiledning om hva som ligger i samtykkekravene.³

Det er særlig kravet om at samtykket skal være frivillig som kan være vanskelig å oppfylle som offentlig myndighet eller arbeidsgiver, siden et av vurderingsmomentene er styrkeforholdet mellom den registrerte og behandlingsansvarlig. Normalt kan ikke samtykke brukes som

³ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/samtykke/>

behandlingsgrunnlag når behandlingsansvarlig er offentlig myndighet eller arbeidsgiver, fordi den registrerte er i et avhengighetsforhold til behandlingsansvarlig.

3.5 Nærmere om berettiget interesse

For dette behandlingsgrunnlaget kreves det at virksomheten må gjennomføre en interesseavveining mellom virksomhetens berettigede interesse og den registrertes interesser, grunnleggende rettigheter og friheter, og særlig når det er snakk om barn.

GDPR angir ikke hvilke momenter som skal vurderes i en slik interesseavveining. Virksomheten må veie sin egen interesse i behandlingen opp mot personvernkonsekvensene for den registrerte. Hvis virksomheten ikke har en tungtveiende interesse, kan behandlingen bare skje hvis personvernkonsekvensene for de berørte er små. Jo større personvernulempene er, desto tyngre må virksomhetens interesse veie for å kunne lande på at det er snakk om en berettiget interesse. Virksomheten kan iverksette tiltak som reduserer personvernkonsekvensene.

I sum må det være en balanse mellom personverninngrepet og virksomhetens berettigede interesse, slik at behandlingen er forholdsmessig. Det finnes mer veiledning om hvordan virksomheten kan foreta en slik interesseavveining på Datatilsynets nettside.⁴

4 Viderebehandling av personopplysninger

Viderebehandling av personopplysninger er når behandlingen handler om personopplysninger som allerede er samlet inn for et annet formål, og man planlegger å behandle disse for et nytt formål.

Det er et krav i regelverket at viderebehandling eller gjenbruk er forenlig med det første formålet opplysningene ble samlet inn for. Det er flere momenter som må vurderes for å avgjøre om formålet er forenlig. Hvis en fotballklubb har samlet inn personopplysninger til en medlemsliste, så vil formålet antagelig være å administrere aktivitetene i klubben, f. eks sende ut faktura, gi informasjon om treningstider osv. Det vil ikke være forenlig med dette formålet at medlemslisten brukes til å sende ut reklame for markedsføringsformål (selv om reklamen er for en fotballtur til England). På den annen side kan det være forenlig med det første og opprinnelige formålet hvis medlemslisten brukes til å sende ut informasjon om en bestemt fotballturnering medlemmene bruker å delta på.

4.1 Hvordan gå frem ved viderebehandling av personopplysninger?

Hvis det planlegges å viderebehandle personopplysninger som allerede er samlet inn for et annet formål, må det først vurderes om det nye formålet er forenlig med det opprinnelige formålet. Hvis man etter en vurdering som nedenfor i punkt 4.2 om forenlighetstest kommer til at formålene er forenlige, kan personopplysningene behandles for det nye formålet. Hvis resultatet

⁴ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/nodvendig-for-a-ivareta-legitime-interesser---interesseavveining/>

av vurderingen er at nytt formål er uforenlig, så kan ikke opplysningene behandles for nytt formål. Personopplysningene kan dermed kun behandles innenfor det opprinnelige formål.

Ved vurderingen av om nytt formål er forenlig med opprinnelig formål er det tre ulike utgangspunkter:

1. Nytt formål er åpenbart innenfor det opprinnelige formålet

Dette gjelder blant annet hvis personopplysningene skal behandles for å oppnå det opprinnelige formålet (f. eks en behandling som burde vært påtenkt fra start, men som man overså var nødvendig for å oppnå formålet). Behandlingen bør være vanlig for å oppnå denne type formål. Vanligvis vil det ikke være behov for videre vurderinger i slike tilfeller.

2. Det er ikke åpenbart at nytt formål er innenfor det opprinnelige formålet

Her er gjerne det nye formålet beslektet med det opprinnelige formålet, men matcher ikke helt. Her vil det være behov for en grundigere og mer omfattende vurdering for å avklare forenlighet mellom formålene. Virksomheten må blant annet vurdere om behandling for det nye formålet er noe den registrerte kan forvente i en slik sammenheng. Hvis virksomheten f. eks kommer til at det er en tett forbindelse mellom opprinnelig og nytt formål, vil det i noen tilfeller kunne sies at det er forenlighet mellom formålene og at personopplysningene dermed lovlig kan behandles for nytt formål.

3. Nytt formål er åpenbart ikke innenfor det opprinnelige formålet

Dette vil gjerne være tilfelle der en rimelig person ikke vil forvente at opplysningene behandles for det nye formålet med tanke på hva personopplysningene opprinnelig ble samlet inn for. Det er stor sannsynlighet for at nytt formål ikke er forenlig med opprinnelig formål, og det er sjelden behov for videre vurderinger. Behandlingen for nytt formål kan ikke gjennomføres.

4.2 Forenlighetstest

Vurderingen av om formålet er forenlig med opprinnelig formål, må gjøres konkret fra sak til sak. I GDPR art.6 nr.4 legges det opp til en «forenlighetstest» og bestemmelsen lister opp flere momenter som må vurderes for å bestemme om personopplysningene kan gjenbrukes til et annet formål. I tillegg kan det være andre relevante momenter. Nedenfor følger momentene fra GDPR art. 6.4 som *alltid* må vurderes:

- Hvilken forbindelse det er mellom opprinnelig formål og formålet for viderebehandlingen
- Hvilket nytt formål kan en vanlig person med rimelighet forvente og akseptere at opplysningene blir brukt til, og er det nye formålet et logisk neste steg i behandlingen det er snakk om? Jo mer utydelig forbindelsen er mellom opprinnelig og nytt formål, desto grundigere og mer omfattende vurdering må gjøres av forenligheten. Hvis f. eks et

kommunalt bibliotek samler inn personopplysninger for å administrere lån av bøker ol. vil dette være det opprinnelige formålet. Hvis biblioteket deretter ønsker å bruke de samme personopplysningene til å tilby andre tjenester som ikke er konkret knyttet til utlån av bøker ol. og som er utenfor det den registrerte kan forvente som kunde i et offentlig bibliotek, vil det antagelig ikke være en nær nok forbindelse mellom det nye formålet og opprinnelig formål. Hvilken sammenheng opplysningene er samlet inn i, og der det særlig skal tas hensyn til forholdet mellom de registrerte og den behandlingsansvarlige

- Når sammenhengen skal vurderes bør det sees på forholdet mellom den registrerte og den behandlingsansvarlige. Hva er vanlig praksis og hva kan med rimelighet forventes i et slikt forhold og sammenheng behandlingen av personopplysninger skjer i? Hvis viderebehandlingen er uforventet og overraskende utfra forholdet og sammenhengen, er det større grunn til å si at nytt formål er uforenlig. Det bør også sees på maktbalansen mellom behandlingsansvarlig og den registrerte, og hvor frivillig behandlingen er for den registrerte. Et annet moment som er relevant å vurdere, er informasjonen den registrerte har fått og hvor stor åpenhet det har vært rundt behandlingen. Videre er det slik at hvis opprinnelig formål er tydelig og restriktivt, vil dette kunne legge begrensninger i viderebehandling. Hvis man har søkt på en konkret stilling i Oslo kommune og gitt fra seg personopplysninger i søknadsprosessen, kan de samme personopplysningene ikke gis videre internt til en annen virksomhet i kommunen som tilfeldigvis leter etter noen med slik kompetanse. Personopplysningene kan kun behandles i rekrutteringsprosessen der den registrerte selv har søkt stillingen.
- ▶ Hvilke personopplysninger det er snakk om, og om det er særlige kategorier (sensitive) personopplysninger eller personopplysninger om straffedommer eller lovovertridelser
 - Jo mer sensitive og beskyttelsesverdige personopplysningene som skal viderebehandles er, desto mer varsom bør man være med å komme til at nytt formål er forenlig med det opprinnelige formålet.
- ▶ Hvilken konsekvens viderebehandlingen kan ha for den registrerte
 - Det bør tas hensyn til både positive og negative konsekvenser viderebehandlingen kan ha for den registrerte, og det bør også vurderes om formålet kan oppnås på en annen måte hvis dette har mindre negative konsekvenser for den registrerte. Kan viderebehandlingen føre til at den registrerte blir irritert, stresset eller føler at han mister kontroll over egne personopplysninger? Blir personopplysningene tilgjengeliggjort for flere? Skal personopplysningene sammenstilles med andre opplysninger? Jo mer uforutsigbare og negative konsekvensene er for den registrerte, desto mer sannsynlig er det at nytt formål ikke er forenlig.
- ▶ Om det foreligger nødvendige garantier
 - Er det gjennomført tiltak for å sikre at personopplysningene behandles på en lovlig og rettfærdig måte, samt tiltak for å forebygge at viderebehandlingen får unødvendige konsekvenser for den registrerte? Dette kan være tekniske eller organisatoriske tiltak. Et eksempel på tiltak er at personopplysningene gjøres mindre identifiserbare. Et annet tiltak kan være at den registrerte gis mer informasjon eller får muligheten til å si nei til viderebehandlingen.

Det kan også være andre relevante momenter som bør være med i vurderingen av forenlighet, men det må som sagt *alltid* tas hensyn til momentene i listen over.

Hvis man etter en forenlighetstest som over kommer til at det nye formålet for viderebehandlingen ikke er forenlig med det opprinnelige formålet, så kan ikke personopplysningene behandles for det nye formålet. En slik behandling vil ikke være lovlig. Det betyr ikke at all behandling må stoppe, man kan fortsette å behandle personopplysningene innenfor det opprinnelige formålet. Det vil være i strid med formålsbegrensningsprinsippet å finne et nytt behandlingsgrunnlag for det nye formålet ved uforenlighet. Siden hensynet bak formålsbegrensning nettopp er å hindre formålsutglidning eller behandling utenfor formålet, kan man ikke finne nytt behandlingsgrunnlag for et uforenlig formål.

Husk at for å kunne viderebehandle personopplysninger for et nytt formål, så må man være behandlingsansvarlig også for behandlingen for det opprinnelige formålet. Hvis det er snakk om en annen behandlingsansvarlig må virksomheten finne sitt eget behandlingsgrunnlag og samle inn opplysningene på nytt hvis man har behandlingsgrunnlag

Siden formålet med behandlingen er en type informasjon den registrerte har krav på å få, bør det gis oppdatert informasjon til den registrerte om det nye formålet. Dette kan f. eks gjøres ved å oppdatere personvernerklæringen. Behandlingsoversikten/protokoll bør også oppdateres med nytt formål.

Husk også at det er egne regler for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål. Om disse formålene er forenlige med opprinnelig formål må vurderes konkret.

5 Oppsummering

Sjekkliste ved vurdering av behandlingsgrunnlag:

- ✓ Lag en tydelig formålsbeskrivelse
- ✓ Finn et dekkende behandlingsgrunnlag for personopplysninger i GDPR art.6
- ✓ Hvis det skal behandles særlige kategorier personopplysninger, finn et unntak i GDPR art.9 og sjekk at det ikke finnes forbehold som gjør at bestemmelsen ikke kan brukes
- ✓ Sjekk om det er behov for å finne supplerende rettsgrunnlag.
- ✓ Hvis personopplysningene allerede er samlet inn og skal brukes til et nytt formål, gjennomfør en forenlighetstest.
- ✓ Lag dokumentasjon for vurderingene.