Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Personvernombud

Støttedokument
Faktaark nr. 35
Versjon: 3.0
Dato: 12.03.2019

Formål	Å sikre riktig saksgang ved utpeking av personvernombud, å sikre at ledelsen legger til rette for at personvernombudet kan utføre sine lovpålagte oppgaver, og å bevisstgjøre ledelsen på dets ansvar som dataansvarlig.		
Ansvar	Personvernombudet er en rådgiver til ledelsen. Dataansvaret ligger alltid hos ledelsen, ikke hos ombudet. Virksomhetens ledelse er ansvarlig for å utpeke et personvernombud, og sørge for at ombudet har de ressurser og virkemidler som er nødvendige for å kunne ivareta oppgavene som ligger til ombudet. Personvernombudet skal gjennomføre oppgavene som ligger til rollen, og sørge for at de blir fulgt		
Gjennomføring	Ved etablering av personvernombud og etter at et personvernombud formelt er meldt inn til Datatilsynet.		
Målgruppe Dette faktaarket er spesielt relevant for:	☐ Leverandør ☐ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder/ sikkerhetskoordinator ☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☒ Personvernombud
Omfang	Alle virksomheter som behandler helse- og personopplysninger som har, eller som skal etablere et personvernombud.		
Hjemmel	• Personvernforordningen artikkel 37-39 • Personopplysningsloven §§ 8-10, og kapittel 5		
Referanser	• Datatilsynets veiledning og innmelding av personvernombud: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/ • Tips til nye ombud: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/tips-til-personvernombud/ • Artikkel 29 gruppen: retningslinjer for databeskyttelsesrådgivere		

Innholdet i dokumentet er gjennomgått og oppdatert ut fra Normen 5.3, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning

Om utpeking av personvernombud

Virksomhetens øverste ledelse skal sørge for at det utpekes personvernombud. Dette gjelder for offentlige virksomheter og for private virksomheter i helsesektoren som behandler helse- og personopplysninger i stor skala.

Personvernombudet kan være ansatt internt i virksomheten eller være en ekstern part som utfører oppgaver på grunnlag av en tjenesteavtale. Ombudet skal utpekes på grunnlag av faglige kvalifikasjoner og sin dybdekunnskap om personvernlovgivningen og praksis på området. Personvernombudet skal være uavhengig i sin stilling, og skal rapportere direkte til det høyeste ledelsesnivået hos dataansvarlig eller databehandler.

Vurdering av behovet for personvernombud i mindre private virksomheter [1]

Det er fremdeles noe uklart hvorvidt mindre private virksomheter i sektoren trenger et personvernombud. Datatilsynet nevner fastleger som kun behandler opplysninger for et begrenset antall pasienter som et eksempel der det ikke kreves personvernombud. Tilsynet har utarbeidet en trinn-for-trinn veileder for virksomheter som er usikre på om de må ha eget personvernombud:

[1] Sekretariatet for Normen arbeider i samarbeid med sektoren, for å fastsette krav for hvor store/små en privat virksomhet skal være, før de plikter å ha et eget personvernombud.

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/trinn-for-trinn-veileder/. For mindre private virksomheter i sektoren kan det være usikkerhet knyttet til behandlinger i "stor skala" (behandlinger av personopplysninger i stort omfang) som kan være utgangspunktet for hvorvidt en privat virksomhet plikter å ha et eget ombud eller ikke. Dette dreier seg om behandling av betydelig mengde personopplysninger som kan påvirke et stort antall registrerte. Følgende faktorer bør vektlegges når det tas stilling til om virksomheten behandler personopplysninger i stor skala:

- Antall registrerte involverte (i tall eller prosentandel av utvalget)
- Volumet av data (antall variabler, detaljeringsgrad)
- Lagringstid (kort, tidsavgrenset, permanent)
- Geografisk omfang (lokalt, regionalt, nasjonalt internasjonalt, globalt)

Eksempler på aktører som foretar behandling av personopplysninger i stor skala er sykehus, offentlige transportsystemer i en by, banker, forsikringsselskaper, søkemotorer på internett og internett- og teletilbydere. Eksempler på aktører som ikke vil komme inn under begrepet som stor skala er fastleger eller advokater som kun behandler opplysninger for et **begrenset** antall pasienter eller kunder.

Dersom virksomheten ikke er pålagt å ha et ombud, anbefaler vi at virksomheten dokumenterer de vurderinger som har blitt gjort dersom det ikke blir opprettet en stilling for personvernombud.
Alle virksomheter står fritt til å utpeke et ombud, selv om de ikke er pålagt å ha ombud etter kriteriene i personvernforordningen artikkel 37.

Internt vs. eksternt personvernombud
Personvernombudet kan enten være ansatt i virksomheten (internt ombud) eller leid inn (eksternt ombud). Et internt ombud kan ha hele eller en del av sin arbeidstid dedikert til stilling. Stillingen som personvernombud skal alltid være uavhengig, med mulighet til å rapportere til øverste ledelse. Fordelen med et internt ombud kan være at vedkommende kjenner virksomheten og sektoren godt.

Et eksternt ombud leies inn, og rollen reguleres i separat privatrettslig avtale mellom virksomheten og ombudet (betingelser som varighet, honorar, omfang, oppgaver mv.).. Fordelen med et eksternt ombud kan være at vedkommende vil kunne se oppgaver med andre øyne, og ikke være farget av virksomheten.

Personvernombudets stilling etter personvernforordningen artikkel 38
Personvernombudet er en rådgiver til ledelsen. Dataansvaret ligger alltid hos ledelsen, ikke hos ombudet.

Dataansvarlig og databehandler skal sikre at personvernombudet involveres i alle spørsmål som gjelder vern av personopplysninger. De skal støtte personvernombudet i utførelsen av sitt virke ved at det gis ressurser og virkemidler som er nødvendig for å utføre de lovpålagte oppgavene, samt at de skal gi tilgang til personopplysninger og behandlingsaktivitetene som gjør det mulig for ombudet å opprettholde sin dybdekunnskap. De skal sikre at ombudet ikke mottar instrukser om utførelsen av sine lovpålagte oppgaver, og de kan ikke avsette eller straffe ombudet for å utføre sine oppgaver. Personvernombudet skal rapportere til høyeste ledelsesnivå hos både dataansvarlig og databehandler.

Personvernombudet skal utnevnes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området, samt evne til å utføre oppgavene som pålegges et ombud (se under). Ombudet skal sikres tilstrekkelige ressurser og arbeidskapasitet.

Dersom ombudet tillegges andre oppgaver, må det sikres at dette ikke er til hinder for at ombudet kan utøve den uavhengighet som skal ligge til rollen. Personvernombudet må ikke ha interessekonflikt med eventuelle andre roller som vedkommende innehar i virksomheten. Personvernombudet kan ha andre oppgaver og plikter, men dataansvarlig må sikre at andre oppgaver og plikter ikke medfører en interessekonflikt. Det betyr blant annet at personvernombudet ikke kan ha en stilling i virksomheten som innebærer at vedkommende fastsetter databehandlingens formål og bestemmer virkemidlene, eller

at det tillegges oppgaver som kommer i konflikt med plikten til å kontrollere etterlevelsen av personvernreglene. Hvert enkelt tilfelle må overveies. F.eks. kan motstridende stillinger i virksomheten være administrerende direktør, IKT-direktør, økonomidirektør, personalsjef, foretaksjurist eller kommuneadvokat. Virksomheten bør utarbeide interne rutiner for å unngå interessekonflikter.

Personvernombudet har taushetsplikt og en plikt til konfidensiell behandling av opplysninger ved utførsel av sine oppgaver (også overfor dataansvarlig og andre ansatte i virksomheten) etter personvernforordningens artikkel 38 nr. 5 og personopplysningsloven § 18. Dette vil være gjeldende der ombudet får adgang til eller kjennskap til det de i sin utførelse av oppgaver får vite om; personlige forhold, tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger, og forretningshemmeligheter (eller når det er av slik art at andre kan utnytte dem i sin næringsvirksomhet), sikkerhetstiltak etter artikkel 32, eller enkeltpersoners varsling om overtredelser av personvernforordningen.

Taushetsplikten gjelder ikke dersom ombudet får samtykke fra den opplysningene gjelder til å legge frem, eller dette er nødvendig for gjennomføring av ombudets lovpålagte oppgaver. Taushetsplikten skal gjelde etter ombudet har avsluttet tjenesten eller arbeidet.

Personvernombudet kan få kunnskap gjennom Datatilsynets tilbud om informasjon og rådgiving gjennom veiledningsmateriell. Datatilsynet har gitt ut en egen veileder som gjelder alle personvernombud. I denne veilederen er det ikke stilt spesifikke formalkrav til personvernombudet. Det bør legges til rette for at personvernombudene kan organisere kurs, workshop eller nettverksmøter med andre personvernombud i helsesektoren.

Datatilsynet forvalter registeret over personvernombud i Norge. Personvernombudet registreres gjennom Altinn. Selv om et ombud er oppnevnt, har den dataansvarlige det formelle ansvaret for behandlingen av helse- og personopplysninger, og for at Normens krav etterleves. Personvernombudet skal ikke beslutte behandlinger av personopplysninger eller metode/verktøy for slike behandlinger, men kan fungere som rådgiver i en slik prosess.

Personvernombud i helsesektoren
Kjennskap til helseområdet og relevante krav i helselovgivningen (eks. dokumentasjonsplikt og relevante pasient- og brukerrettigheter) og virksomheten personvernombudet er ombud for, bør legges vekt på ved utpeking. Personvernombudet bør også ha en god forståelse og kjennskap til behandlingsaktivitetene som utføres, informasjonssystemene som benyttes og datasikkerheten i virksomheten, samt dataansvarliges behov for databeskyttelse.

I større virksomheter bør det oppnevnes en stedfordrer for personvernombudet når personvernombudet ikke er til stede i virksomheten (eks. ved sykdom og ferier). I tillegg bør det vurderes om det er nødvendig med rådgivere som kan bistå ombudet.

Personvernombudets oppgaver etter forordningens artikkel 39
Følgende punkter er kontinuerlige plikter etter personvernforordningens artikkel 39 som lister opp minimumsoppgavene et personvernombud skal ha:

a) Informere og gi råd til dataansvarlig eller databehandler og de ansatte som utfører behandlingene om kravene i forordningen, personopplysningsloven og helserettens bestemmelser om personvern og informasjonssikkerhet
b) Kontrollere overholdelsen av personvernregelverket og helserettens bestemmelser om personvern og informasjonssikkerhet, samt virksomhetens egne interne retningslinjer for personvern
c) Ombudet skal gi råd om vurdering av personvernkonsekvenser (DPIA). Det er dataansvarlig som har ansvaret for at slike vurderinger gjennomføres. Dataansvarlig kan f.eks. be om råd om:
    - om det er behov for å utføre en vurdering av personvernkonsekvenser

- hvilken metode som skal benyttes
- konsekvensvurderingen skal gjøres internt eller ved hjelp av eksterne krefter
- hvilke sikkerhetstiltak (tekniske og organisatoriske) som bør tas for å minimere risiko
- hvorvidt konsekvensvurderingene er blitt gjennomført på riktig måte, og om konklusjonene er i tråd med regelverket

d) Samarbeide med Datatilsynet og fungere som kontaktpunkt for tilsynet ved eventuelle spørsmål. Det er personvernombudet som skal legge til rette for at Datatilsynet får den informasjonen det trenger for å utføre sine oppgaver og plikter. Ombudet skal bistå de registrerte med å ivareta deres rettigheter dersom de kontakter personvernombudet med spørsmål knyttet til virksomhetens behandling av personopplysninger

e) Prioritere innsats der personvernrisikoen er høyest. I sine oppgaver skal ombudet ta hensyn til risikoene forbundet med behandlingsaktivitetene i lys av behandlingens art, omfang, formål og sammenheng. Det betyr at ombudet må prioritere områder hvor risikoen for personvernet er høyest.

Personvernombudets anbefalte oppgaver i helsesektoren

Normen *anbefaler* følgende oppgaver knyttet til personvernombudet i helsesektoren:

a) gjennomføre minst to årlige rapporteringer til dataansvarlig/ledelse (ledelsens gjennomgang):
- rapporteringen skal inneholde status (siden forrige rapportering) på følgende
- informere om status for bruk av internkontrollsystemet og evt. avvik fra kravene. Dette er særlig viktig ved endringer i elektroniske pasient- og journalsystemer.
- kort oppsummering av bistand gitt registrerte
- avvik og brudd på reglene for behandling av helse- og personopplysninger
- informere om evt. «nyheter» innen temaet personvern og informasjonssikkerhet, herunder endringer i kravene etter gjeldende regelverk eller i Normen med tilhørende faktaark
- gi råd og anbefalinger for å sikre korrekt behandling av helse- og personopplysninger i virksomheten, herunder gi status på evt. løpende tiltak for å sikre dette

c) både ledelsen ved dataansvarlig og personvernombudet kan stille krav til oppfølging på temaene i rapporteringspunktene

d) bistå og tilrettelegge arbeidet knyttet til ledelsens gjennomgang (årlig)

Juridiske ansvarsforhold

Følgende juridiske ansvarsforhold gjelder ved opprettelse av et personvernombud i virksomheten:
- dataansvarlig er juridisk ansvarlig for behandlingen av helse- og personopplysninger i den aktuelle virksomheten
- ombudet er avtalerettslig forpliktet overfor dataansvarlig i kraft av stillingsinstruks/avtale, se eksempel. Det er viktig å bemerke at stillingsinstruksen/avtalen ikke kan begrense personvernombudets uavhengighet.
- En avslutning av arbeidsforholdet mellom dataansvarlig og personvernombudet kan ikke begrunnes i hvordan personvernombudet løser sine arbeidsoppgaver. Personvernombud har et sterkere oppsigelsesvern enn vanlige arbeidstakere.

Handling/utførelse

Nr.	Aktivitet/beskrivelse
1	**Vurdere opprettelse av personvernombud** Et beslutningsgrunnlag for opprettelse av et personvernombud kan innhentes ved: a) Datatilsynet gir råd og informasjon om ombudsrollen b) Datatilsynet har til enhver tid en kontaktperson for hjelp og veiledning ifm vurdering av opprettelse av personvernombud
2	**Identifisere og velge kandidat** Vurdér følgende når beslutning om opprettelse av personvernombud er tatt: a) vurdér og beslutt omfanget personvernombudsrollen (se innledning) b) vurdér og beslutt arbeidsoppgavene til personvernombudet (se innledning) c) utform skisse til stillingsinstruks eller kontrakt (se eksempel)

Nr.	Aktivitet/beskrivelse
	d) identifiser og vurdér intern eller ekstern kandidat, med bakgrunn i omfang, arbeidsoppgaver og kompetansekrav (se innledning) e) vurdere om kandidaten er motivert og kvalifisert for oppgaven som personvernombud på bakgrunn av definert omfang, arbeidsoppgaver og kompetansekrav f) velg og beslutt personvernombud
	Hvis valg av *internt* personvernombud a) utform stillingsinstruks (se eksempel) med beskrivelse av krav til omfang og arbeidsoppgaver, tilpass evt. ytterligere iht. virksomhetens særlige behov b) Vurdere interessekonflikter stillingen kan få i kombinasjon med andre stillinger/oppgaver i virksomheten (f.eks. personvernombud i kombinasjon med administrerende direktør, IKT-direktør, økonomidirektør, personalsjef, foretaksjurist, kommuneadvokat mv.) Omfanget av ulike stillinger/oppgaver må tas med som vurderingsgrunnlag).
	Hvis valg av *eksternt* personvernombud a) utform avtale (se eksempel) med beskrivelse av krav til omfang og arbeidsoppgaver, tilpass evt. ytterligere iht. virksomhetens særlige behov b) avklar betingelser (varighet, honorar) c) signer avtale med eksternt personvernombud
	Organisatorisk plassering av ombudet a) avklare og beslutte hvor personvernombudet skal forankres i organisasjonen (f.eks. i stab, administrasjon, sikkerhetsledelsen, sammen med andre interne ombud (f.eks. verneombud mv.)) Utgangspunktet er alltid at ombudet skal være uavhengig, og rapportere til øverste ledelse i virksomheten.
	Melde inn personvernombudet til Datatilsynet a) Registrere ombudets kontaktopplysninger hos Datatilsynet via Altinn. Dette gjelder både virksomheter som er pålagt å ha ombud og virksomheter som oppretter ombud frivillig.
3	**Presentasjon av rollen internt** Personvernombudet skal markedsføre rollen internt. Som første tre aktiviteter kan personvernombudet: a) etablere f.eks. egne sider på intranett b) etablere e-post til ombudet, f.eks. personvernombud@virksomheten.no hvor spørsmål og andre henvendelser kan rettes c) presentere seg og sine oppgaver og sitt ansvar i interne fora som f.eks. interne avdelingsmøter og faggrupper
	Personvernombud – løpende ansvar a) Personvernombudet plikter å følge opp det definerte ansvaret iht. stillingsinstruks/kontrakt. Dette inkluderer de oppgavene som er beskrevet i dette faktaarket. b) Personvernombudet og virksomheten plikter å ivareta retningslinjene for de juridiske ansvarsforholdene (se innledning).