

 <p>Norm for informasjonssikkerhet www.normen.no</p>	<p>Utgitt med støtte av:</p> 
<h2 style="text-align: center;">Personvernombud</h2>	<p>Støttedokument Faktaark nr. 35 Versjon: 2.1 Dato: 15.12.2010</p>

<p>Målgruppe</p> <p>Dette faktaarket er spesielt relevant for:</p>	<input type="checkbox"/> Leverandør <input type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/ sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input checked="" type="checkbox"/> Personvernombud
<p>Ansvar</p>	<p>Virksomhetens ledelse er ansvarlig for opprettelse av personvernombud og for oppfølging/løpende vurdering av ombudet. Personvernombudet er ansvarlig for at oppgavene som ligger til rollen blir fulgt. Selve databehandlingsansvaret ligger likevel alltid hos ledelsen, ikke hos ombudet.</p>		
<p>Gjennomføring</p>	<p>Ved etablering av personvernombudsrollen og etter at et personvernombud formelt er pekt ut av Datatilsynet.</p>		
<p>Formål</p>	<p>Å sikre riktig saksgang ved utnevning av ombud, å sikre at ledelsen har definert klare og relevante arbeidsoppgaver og ansvarsområder for ombudet, og å bevisstgjøre ledelsen på at den har det formelle databehandlingsansvaret, selv om det er pekt ut et ombud.</p>		
<p>Omfang</p>	<p>Alle virksomheter som behandler helse- og personopplysninger og som skal etablere/vurderer å etablere et personvernombud.</p>		
<p>Hjemmel</p>	<ul style="list-style-type: none"> • EUs personverndirektiv (som gjelder hele EØS-området) • personopplysningsloven kapittel VIII • personopplysningsforskriften § 7-12 		
<p>Referanser</p>	<ul style="list-style-type: none"> • Veileder for personvernombud/søknadsskjema for opprettelse av personvernombud/standard godkjennelsesvedtak for personvernombud: http://www.datatilsynet.no • Om personvern – drevet av personvernombudet ved UiO: http://www.personvern.uio.no • Kompetansesenter for personvern v/Ullevål universitetssykehus: http://www.uus.no/personvern 		

Om personvernombud

Alle helsevirksomheter behandler daglig helse- og personopplysninger, foretar forskning og mottar spørsmål, klager, krav om innsyn eller andre henvendelser om informasjonssikkerhet og personvern fra pasienter, pårørende eller egne ansatte. For en del virksomheter kan det være en god løsning å opprette et personvernombud for å imøtekomme dette.

Opprettelsen av rollen som personvernombud er frivillig. Etablering av rollen gir den fordelen at ansvar og aktiviteter - likevel tillagt virksomheten - blir formalisert. Virksomheten er fritatt meldeplikten overfor Datatilsynet, meldingene formidles i stedet til personvernombudet. I tillegg vil personvernombudet kunne få kunnskap og kompetanse gjennom Datatilsynets tilbud om seminar, informasjon og rådgiving. På seminarene presenteres og diskuteres utfordringer på tvers av virksomheter som har etablert ordningen. Datatilsynet har gitt ut en egen veileder som gjelder alle personvernombud. I denne veilederen er det ikke stilt spesifikke formalkrav til personvernombudet. Imidlertid bør - med bakgrunn i helsesektorens særlige karakter - de kompetanseanbefalinger som er angitt i dette faktaarket, benyttes ved oppnevning av et personvernombud i virksomheten.

Et personvernombud er en formelt oppnevnt kontakt for personvern og informasjonssikkerhet **internt** mot databehandlingsansvarlig (virksomhetens ledelse) og ansatte og **eksternt** mot Datatilsynet og den registrerte (pasienter og egne ansatte). Ombudet skal håndtere henvendelser fra, og kan være et bindeledd mellom, bl.a. følgende aktører: egen virksomhet/organisasjon, den registrerte, Datatilsynet, forskningsmiljøer, andre helsevirksomheter og publikum. Ombudet skal være en ressursperson som har kunnskap om virksomheten og behandlingen av helse- og personopplysninger.

Datatilsynet forvalter ordningen. Både virksomheten og personvernombudet er forpliktet til å følge opp de oppgavene som følger av Datatilsynets oppnevningsvedtak (se nedenfor om fremgangsmåten). Selv om et ombud er oppnevnt, har den databehandlingsansvarlige det formelle ansvaret for behandlingen av helse- og personopplysninger, og for at Normens krav etterleves.

Anbefalte krav for ombud i helsesektoren

Det foreligger ingen formelle kompetansekrav til personvernombudet, men det forutsettes og det er av betydning at ombud i helsesektoren:

- blir sikret tilstrekkelige ressurser og arbeidskapasitet, og at personvernombudet har bred kompetanse i organisasjonen og virksomheten

Videre bør et personvernombud utvikle:

- god forståelse for utfordringene knyttet til personvern og informasjonssikkerhet i helsesektoren
- generell kunnskap om og interesse for bruk av it-verktøy i arbeidsprosessene
- kunnskap om bruk av elektroniske pasientsystemer (gjelder virksomheter som har slike systemer)
- god kjennskap til personopplysningsloven, helseregisterloven, helsepersonelloven og annet relevant lovverk
- god kjennskap til Normen, herunder faktaark

Anbefalingene er nyttige for å kunne sette seg inn i og forstå hvordan helse- og personopplysninger faktisk behandles i egen virksomhet og hvordan de skal behandles.

Internt vs. eksternt personvernombud

Personvernombudet er enten ansatt i virksomheten (internt ombud) eller leid inn (eksternt ombud). Store virksomheter bør ha et internt ombud, små virksomheter kan vurdere å peke ut et eksternt ombud. Et internt ombud har hele eller en del av sin arbeidstid dedikert til rollen. Et eksternt ombud leies inn, og rollen (betingelser som varighet, honorar, omfang, oppgaver mv.) reguleres i separat privatrettslig avtale mellom virksomheten og ombudet. Forslag til elementer i en avtale for et personvernombud (internt eller eksternt) finnes i vedlagte eksempel.

Omfanget av personvernombudsrollen i helsesektoren

Datatilsynets veileder for personvernombud gir standard veiledning for alle virksomheter og bransjer. For personvernombud i helsevirksomheter gis, i tillegg til tilsynets veiledning, nedenstående anbefalinger. Det presiseres at organiseringen er avhengig av lokale forhold og må vurderes konkret. Anbefalingene er derfor kun veiledende og virksomheten har følgelig stor frihet til å organisere personvernombudsrollen etter eget behov.

a) Antall personvernombud i samme helsevirksomhet:

- Formelt er det den databehandlingsansvarlige som selv bestemmer om det skal utnevnes ett eller flere personvernombud i virksomheten. Som utgangspunkt anbefales det å ha kun ett personvernombud i helsevirksomheter. Personvernombudet kan imidlertid organisere det praktiske arbeidet slik at flere personer med ulike ansvar- og kompetanseområder er involvert.

b) Antall virksomheter for samme personvernombud:

- Formelt kan et personvernombud være ombud for flere virksomheter. Det anbefales likevel å begrense antall virksomheter av hensyn til kompetansekravene knyttet til arbeidskapasitet og innsikt i organisasjon og virksomhet.

c) Omfanget av ombudets arbeidsområde:

- Rollen som ombud skal omfatte alle behandlinger av helse- og personopplysninger i virksomheten og hos databehandlere.

Personvernombudets oppgaver etter Datatilsynets standardvedtak

Følgende punkter er kontinuerlige plikter etter Datatilsynets standardvedtak; ombudets øvrige oppgaver og plikter må spesifiseres i den enkelte stillingsinstruks eller avtale:

- *motta meldinger*: påse at behandlinger av personopplysninger blir meldt til ombudet, og at meldingene inneholder korrekte og tilstrekkelige opplysninger
- *føre fortegnelse*: føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene gitt i meldingene
- *internkontroll*: påse at databehandlingsansvarlig har et system for internkontroll som tilfredsstiller kravene i personopplysningsloven
- *bistå de registrerte*: bistå de registrerte med å ivareta deres rettigheter etter reglene om behandling av personopplysninger
- *påpeke brudd på regler*: ombudet skal varsle om brudd på reglene for behandling av helse- og personopplysninger overfor databehandlingsansvarlig, og i alvorlige tilfeller bistå ledelsen med å orientere Datatilsynet
- *gi opplysninger til Datatilsynet*: ombudet skal gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker
- *holde seg orientert*: ombudet skal være faglig orientert om utviklingen innen relevante personvernspørsmål
- *gi råd og veiledning*: ombudet er en ressursperson og skal gi råd og veiledning til databehandlingsansvarlige i egen virksomhet

Personvernombudets oppgaver i helsesektoren

I tillegg til oppgavene som fremgår av Datatilsynets vedtak, bør følgende gjelde:

- a) gjennomføre minst to årlige rapporteringer til databehandlingsansvarlig/ledelse
- b) rapporteringen skal inneholde status (siden forrige rapportering) på følgende (iht.

personvernombudets oppgaver etter Datatilsynets standardvedtak):

- antall innkommende meldinger (om meldepliktige behandlinger) i inneværende periode, status på foreliggende meldinger og evt. alvorlige avvik
- oversikt over behandlingene av helse- og personopplysninger som finner sted i virksomheten
- oversikt over vesentlige avvik og korrigerende tiltak som er iverksatt
- 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
- brudd på reglene for behandling av helse- og personopplysninger
- kort oppsummering av evt. bistand gitt til Datatilsynet
- 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 databehandlingsansvarlig 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:

- databehandlingsansvarlig er juridisk ansvarlig for behandlingen av helse- og personopplysninger i den aktuelle virksomheten
- ombudet er avtalerettslig forpliktet overfor databehandlingsansvarlig i kraft av stillingsinstruks/avtale, se eksempel

- databehandlingsansvarlig kan avslutte avtalen med personvernombudet basert på vanlig avtalerett
- dersom Datatilsynet ikke er fornøyd med måten personvernombudet skjøtter sine oppgaver på, kan dette medføre at unntaket fra meldeplikten blir trukket tilbake. I alvorlige tilfeller kan Datatilsynet trekke tilbake godkjenningen av ombudet.

Handling/utførelse

Nr.	Aktivitet/beskrivelse
1	<p>Vurdere opprettelse av rollen som personvernombud</p> <p>Et beslutningsgrunnlag for opprettelse av et personvernombud kan innhentes ved:</p> <ol style="list-style-type: none"> Datatilsynet gir råd og informasjon om ombudsrollen Datatilsynet har til enhver tid en kontaktperson for hjelp og veiledning ifm vurdering av opprettelse av personvernombud
2	<p>Identifisere og velge kandidat</p> <p>Vurdér følgende når beslutning om opprettelse av personvernombud er tatt:</p> <ol style="list-style-type: none"> vurdér og beslutt omfanget personvernombudsrollen (se innledning) vurdér og beslutt arbeidsoppgavene til personvernombudet (se innledning) utform skisse til stillingsinstruks eller kontrakt (se eksempel) identifiser og vurdér intern eller eksternt kandidat, med bakgrunn i omfang, arbeidsoppgaver og kompetansekrav (se innledning) vurdere om kandidaten er motivert og kvalifisert for oppgaven som personvernombud på bakgrunn av definert omfang, arbeidsoppgaver og kompetansekrav velg og beslutt personvernombud <p>Hvis valg av internt personvernombud</p> <ol style="list-style-type: none"> utform stillingsinstruks (se eksempel) med beskrivelse av krav til omfang og arbeidsoppgaver, tilpass evt. ytterligere iht. virksomhetens særlige behov <p>Hvis valg av eksternt personvernombud</p> <ol style="list-style-type: none"> utform avtale (se eksempel) med beskrivelse av krav til omfang og arbeidsoppgaver, tilpass evt. ytterligere iht. virksomhetens særlige behov avklar betingelser (varighet, honorar) skriv avtale med eksternt personvernombud <p>Organisatorisk plassering av ombudet</p> <ol style="list-style-type: none"> avklare og beslutte hvor personvernombudet skal forankres i organisasjonen (f.eks. i stab, administrasjon, sikkerhetsledelsen, sammen med andre interne ombud (f.eks. verneombud m.v.)) <p>Søke Datatilsynet om opprettelse av personvernombud og godkjenning</p> <ol style="list-style-type: none"> benytt standard søknadsskjema for formelt å søke og å få godkjent opprettelse av rollen som personvernombud (se http://www.datatilsynet.no) Datatilsynet gir svar og evt. godkjenner søknad og fritak av meldeplikt gjennom vedtak som beskriver ombudets grunnleggende plikter og oppgaver (svar kan påregnes innen 14 dager)
3	<p>Presentasjon av rollen internt</p> <p>Når positivt svar er gitt av Datatilsynet, skal personvernombudet markedsføre rollen internt. Som første tre aktiviteter kan personvernombudet:</p> <ol style="list-style-type: none"> etablere f.eks. egne sider på intranett etablere e-post til ombudet, f.eks. personvernombud@virksomheten.no hvor spørsmål og andre henvendelser kan rettes presentere seg og sine oppgaver og sitt ansvar i interne fora som f.eks. interne avdelingsmøter og faggrupper <p>Personvernombud - løpende ansvar</p> <ol style="list-style-type: none"> Personvernombudet plikter å følge opp det definerte ansvaret iht. stillingsinstruks/kontrakt. Dette inkluderer de oppgavene som er beskrevet i vedtaket fra Datatilsynet. Personvernombudet og virksomheten plikter å ivareta retningslinjene for de juridiske ansvarsforholdene (se innledning)

Eksempel

Følgende er et eksempel på elementer i en stillingsinstruks/avtale for personvernombud, internt eller eksternt. Stillingsinstruks/avtale må tilpasses etter særskilte behov:

1. VIRKSOMHETEN			
Navn på virksomheten		Org.nr.	
Postadresse		Postnr.	
2. DATABEHANDLINGSANSVARLIG (DAGLIG LEDER)			
Navn			
3. PERSONVERNOMBUD			
Navn			
Stilling (hvis stilling i tillegg til ombudsrollen)			
4. JURIDISKE ANSVARFORHOLD			
Internt personvernombud:			
<ul style="list-style-type: none">• denne stillingsinstruks/avtale kan endres av databehandlingsansvarlig i kraft av styringsretten• databehandlingsansvarlig kan når som helst frita ombudet fra vervet som personvernombud i samsvar med alminnelige arbeidsrettslige regler, melding om at ombudet er blitt fritatt må sendes Datatilsynet• personvernombudet kan frasi seg vervet som personvernombud etter nærmere avtale med databehandlingsansvarlig			
Eksternt personvernombud:			
<ul style="list-style-type: none">• denne stillingsinstruks/avtalen kan endres etter nærmere avtale mellom personvernombudet og databehandlingsansvarlig• databehandlingsansvarlig kan frita personvernombudet fra rollen som ombud etter de oppsigelsesfrister som er avtalt i punkt 6 i denne stillingsinstruks/avtalen• personvernombudet kan frasi seg vervet som personvernombud etter de oppsigelsesfrister som er avtalt i punkt 6 i denne stillingsinstruks/avtalen			
5. OPPGAVER OG PLIKTER FOR PERSONVERNOMBUDET			
Partene er bundet av Datatilsynets vilkår for oppnevningen. Vilkårene fremgår av Datatilsynets vedtak. Vedtaket er lagt ved og inngår som en del av denne avtalen.			
I tillegg til oppgavene som fremgår i vedtaket skal personvernombudet skal følgende gjelde:			
a) gjennomføre minst fire årlige rapporteringer til databehandlingsansvarlig/ledelse			
b) rapporteringen skal inneholde status på følgende områder:			
<ul style="list-style-type: none">• antall innkommende meldinger i inneværende periode, status på foreliggende meldinger og evt. alvorlige avvik• status på fortegnelse over behandlingene av helse- og personopplysninger som finner sted i virksomheten, herunder rapportere om evt. alvorlige avvik• informere om status på internkontrollsystemet og evt. avvik fra kravene. Dette er særlig viktig ved endringer i elektroniske pasient- og journalsystemer.• kort oppsummering av bistand gitt registrerte• brudd på reglene for behandling av helse- og personopplysninger• kort oppsummering av evt. bistand gitt Datatilsynet• informere om evt. 'nyheter' innen temaet personvern og informasjonssikkerhet, herunder endringer i krav og regelverk			

<ul style="list-style-type: none"> • 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 <p>c) både ledelsen ved databehandlingsansvarlig og personvernombudet kan stille krav til oppfølging på temaene i rapporteringspunktene</p>			
6. INTERNT ELLER EKSTERNT PERSONVERNOMBUD (sett kryss)			
<input type="checkbox"/> INTERNT OMBUD	Rollen i % av arbeidstid		
	Øvrige betingelser (bruk evt. eget ark)		
<input type="checkbox"/> EKSTERNT OMBUD	Pris		
	Antall timer som inngår i totalramme		
	Øvrige betingelser (bruk evt. eget ark)		
	Oppsigelse	<Gjensidig oppsigelse med én måneds varsel>	
7. GYLDIGHET			
Denne avtalen gjelder inntil den er erstattet av ny avtale, alternativt inntil personvernombudet ikke lenger har rollen som personvernombud. Hvis avtalen er tidsbegrenset skal dette spesifiseres som følger:			
Vedtaksdato fra Datatilsynet			
Avtalen er gyldig fra (dato)		Avtalen er gyldig til (dato)	
8. STED, DATO OG UNDERSKRIFT			
Personvernombudets underskrift		Databehandlingsansvarliges underskrift	
Sted og dato		Sted og dato	
<i>Denne avtalen er utferdiget i to originaleksemplarer, ett til hver av partene.</i>			