Nye personvernregler i 2018

Hva betyr det for din virksomhet?

I 2018 får Norge nye regler for personvern, når EUs forordning erstatter dagens regelverk. Alle virksomheter som behandler personopplysninger om egne ansatte, kunder, brukere eller andre, må følge de nye reglene.

De nye reglene stiller flere og strengere krav. Ett av dem er kravet om å ha personvernombud.

Mange virksomheter blir pålagt å opprette personvernombud

Datatilsynet har utarbeidet en tolkning av det nye regelverket for håndtering av personvern i Norge. De nye reglene trer i kraft i mai 2018. Datatilsynet oppfordrer alle virksomheter til å opprette personvernombud, uavhengig av om de er pålagt å ha det eller ikke.

Definisjoner for hvilke virksomheter som må opprette personvernombud, finnes i artikkel 37 i forordningen. Påbud om ombudsordning gjelder for alle som i sin virksomhet driver med:

- regelmessig og systematisk monitorering i stor skala av personer
- behandling av sensitive personopplysninger

Definisjon av begreper

Stor skala

Forordningen definerer ikke hva som ligger i begrepet stor skala. Følgende faktorer bør imidlertid tas med i en vurdering av om en behandling er i stor skala, eller ikke:

- antallet personer det behandles opplysninger om
- mengden og omfanget av personopplysningene som blir behandlet
- varigheten av behandlingen det geografiske omfanget av behandlingen

Regelmessig

- Behandlingen av personopplysninger skjer løpende eller jevnlig i en bestemt periode
- Behandlingen gjentas på bestemte tidspunkter

Systematisk

- Behandlingen av personopplysninger skjer etter et system
- Behandlingen er forhåndsbestemt, organisert eller metodisk
- Behandlingen skjer som en del av en generell plan for datainnhenting
- Behandlingen skjer som en del av en strategi

Monitorering

Oppsummert omfatter «monitorering» i denne sammenhengen alle former for sporing og profilering på nettet, inkludert persontilpasset reklame.

Begrepet monitorering begrenses imidlertid ikke bare til aktiviteter på internett. Eksempler på aktiviteter som kan komme inn under begrepet monitorering er:

- drift av et telekommunikasjonsnettverk målrettet e-postreklame

- profilering og vurdering i forbindelse med kredittvurdering
- sporing av lokasjon i mobilapplikasjoner monitorering ved bruk av helsearmbånd kundeklubber eller lojalitetsprogrammer kameraovervåking
- bruk av internettilknyttede enheter, som for eksempel smarte biler, automatiske strømmålere, smarthus og lignende

Sensitive opplysninger/særlige kategorier av personopplysninger (art. 9):

- rasemessig eller etnisk opprinnelse politisk oppfatning religiøs eller filosofisk overbevisning fagforeningsmedlemskap
- behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
- helseopplysninger
- opplysninger om en fysisk persons seksuelle forhold eller seksuelle legning

Straffbare forhold (art. 10):

- personopplysninger i forbindelse med straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak

Datatilsynets anbefalinger

Datatilsynet oppfordrer alle virksomheter som gjør en omfattende innsamling og bruk av personopplysninger, eller som behandler opplysninger som er særlig beskyttelsesverdige, om å opprette et personvernombud. Dette gjelder også de som ikke er pålagt å gjøre det. Vær da oppmerksom på at dersom dere oppretter ombud på frivillig initiativ, vil artiklene 37-39 i forordningen gjelde på lik linje som for lovpålagte ombud. Et personvernombud er, uansett om det er pålagt eller frivillig, utnevnt for alle behandlingene av personopplysninger som skjer i virksomheten.

En virksomhet står selvfølgelig fritt til å ansette eller leie inn arbeidskraft for å ivareta personvernet uten at denne eller disse personene har rollen som personvernombud. I slike tilfeller er det viktig at det kommer tydelig fram, både innad og utad i virksomheten, at tittelen, oppgavene og rollen til disse ikke kan forveksles med et personvernombud.

Må også databehandlere opprette personvernombud?

Både den behandlingsansvarlige og databehandler er pålagt å ha personvernombud hvis kriteriene i artikkel 37 er oppfylt. Avhengig av hvem som oppfyller kriteriene kan det være enten behandlingsansvarlig eller databehandler som er pålagt å ha personvernombud, men det kan også være begge.

Et personvernombud som er utnevnt av en databehandler har også ansvar for de øvrige behandlingene som databehandlervirksomheten er behandlingsansvarlig for (for eksempel IT, personal/HR, logistikk og lignende).

Ett ombud for flere virksomheter?

Et konsern kan oppnevne ett felles personvernombud, forutsatt at alle virksomhetene innen konsernet har enkel tilgang til vedkommende. Det samme kan en forening som Fagpressen gjøre. Flere offentlige myndigheter eller organer kan også utnevne et felles ombud på vegne av flere. Dette forutsetter imidlertid at det er forsvarlig ut fra virksomhetenes struktur og størrelse, og ikke minst ut fra omfang og kompleksitet når det gjelder de personopplysningene som behandles.

Hva er ombudets plikter?

I artikkel 39 gir forordningen en oversikt over hvilke oppgaver et personvernombud skal ha.

Informere og gi råd

Personvernombudet skal gi råd til den behandlingsansvarlige eller databehandleren og til de ansatte som utfører behandlingen av personopplysninger om de forpliktelsene virksomheten har etter personvernlovgivningen.

Kontrollere overholdelsen av personvernregelverket

Ombudet skal kontrollere overholdelsen av forordningen og andre relevante regelverk med personvernbestemmelser, samt virksomhetens egne interne retningslinjer for personvern. Som en del av dette kan ombudet ha følgende oppgaver:

1. samle inn informasjon for å identifisere behandlingsaktiviteter

2. analysere og sjekke at behandlingsaktivitetene er i tråd med regelverket

3. informere, gi råd og anbefalinger for å sikre regelverketterlevelse

4. foreslå ansvarsfordeling for oppgaver knyttet til ivaretakelse av personvernet i virksomheten

5. gjennomføre holdningsskapende arbeid i virksomheten og opplæring av medarbeidere

Selv om personvernombudet har en rolle i å kontrollere etterlevelse etter regelverket, er det fremdeles den behandlingsansvarlige eller databehandleren som er ansvarlig for at personvernlovgivningen følges.

Gi råd om vurdering av personvernkonsekvenser (DPIA)

Personvernombudet skal på anmodning gi råd om vurderingen av personvernkonsekvenser (Data Protection Impact Assessment – DPIA) og kontrollere gjennomføringen av konsekvensvurderingene. Det er den behandlingsansvarlige, ikke personvernombudet, som har ansvaret for at slike

vurderinger gjennomføres. Ombudet kan imidlertid ha en viktig rolle med å bistå den behandlingsansvarlige i disse vurderingene.

Artikkel 35 i forordningen pålegger behandlingsansvarlige å be om råd fra ombudet når man skal utføre en konsekvensvurdering. Den behandlingsansvarlige kan be om råd om følgende tema:

1. om det er behov for å utføre en vurdering av personvernkonsekvenser

2. hvilken metode som skal benyttes

3. om konsekvensvurderingen skal gjøres internt eller ved hjelp av eksterne krefter

4. hvilke sikkerhetstiltak (tekniske og organisatoriske) som bør tas for å minimere risiko

5. hvorvidt konsekvensvurderingene er blitt gjennomført på riktig måte, og om konklusjonene er i tråd med regelverket

Samarbeide med Datatilsynet og fungere som kontaktpunkt

Personvernombudet skal samarbeide med datatilsynsmyndigheten og fungere som et kontaktpunkt for tilsynet ved spørsmål. Ved behov skal ombudet også kunne rådføre seg med tilsynet. Disse oppgavene understreker ombudets rolle som kontaktpunkt mellom virksomheten og tilsynsmyndigheten. Ombudet skal legge til rette for at tilsynet får den informasjonen det trenger for å utføre sine oppgaver og plikter, for eksempel i forbindelse med sin kontrollvirksomhet.

De registrerte skal på sin side kunne kontakte personvernombudet om alle spørsmål knyttet til behandling av deres opplysninger, og om utøvelsen av rettighetene de har i henhold til personvernforordningen.

Prioriter innsatsen dit hvor personvernrisikoen er høyest

Forordningen forutsetter at personvernombudet tar hensyn til risikoene

forbundet med behandlingsaktivitetene sett i lys av behandlingens art, omfang, formål og sammenhengen den utføres i. Dette betyr at innsatsen fra personvernombudet sin side naturlig nok i hovedsak bør rettes mot områder hvor risikoen for personvernet vurderes å være høyest.

Bidra til å få oversikt over behandlingene

Artikkel 30 i forordningen pålegger den behandlingsansvarlige eller databehandler å føre en oversikt over hvilke behandlinger av personopplysninger virksomheten har.

Den behandlingsansvarlige kan bestemme å gi ombudet flere oppgaver, så lenge det ikke oppstår interessekonflikt. Det å etablere en slik oversikt er en oppgave som ofte vil bli delegert til personvernombudet. En slik oversikt er da også et viktig verktøy for at personvernombudet skal kunne utføre sine oppgaver.