Om Spør advokaten

Jane Wesenberg er advokat og partner i EY Law. Hun arbeider særlig med arbeidsrett, personvern, petroleumsrett, forvaltningsrett og offentlige anskaffelser. EY Law tilbyr tjenester innen et bredt spekter av forretningsjus, og i denne spalten vil Jane svare på spørsmål knyttet til hele EY Laws fagområde.
Har du spørsmål som også kan være av interesse for Revisjon og regnskaps lesere, kan disse sendes: jane.wesenberg@no.ey.com. i utgangspunktet vil kun spørsmål som kommer på trykk bli besvart.

Personvernombud og sanksjoner i ny personvernforordning

EUs forordning om behandling av personopplysninger – General Data Protection Regulation (GDPR) – trer i kraft mai 2018. Den inneholder blant annet regler om personvernombud og viktige endringer i sanksjonssystemet.

Personvernombud pålegges

Personvernombud er i dagens regelverk definert som en «uavhengig» person i en virksomhet «som har som oppgave å sikre at den behandlingsansvarlige[1] følger personopplysningsloven med forskrift». Ordningen med personvernombud er i dag frivillig, og ment å forenkle overholdelsen av reglene om meldeplikt for virksomheter som behandler personopplysninger i utstrakt grad. I tillegg skaper ordningen et tettere samarbeid mellom virksomhetene og Datatilsynet, fordi personvernombudet opererer som fast kontaktpunkt dem imellom. Personvernombudet utpekes av virksomheten, men må godkjennes av Datatilsynet.

En rekke typer behandling av personopplysninger utløser meldeplikt til Datatilsynet. Dersom en virksomhet har et godkjent personvernombud, er det tilstrekkelig å sende slik melding til personvernombudet. Personvernombudet har deretter plikt til å føre en oversikt over de opplysningene som ellers må meldes til Datatilsynet i samsvar med personopplysningsloven § 32. Dette gjelder både for den alminnelige meldeplikten etter personopplysningsforskriften § 7–12, og i tilfellene der det er meldeplikt som unntak fra konsesjonsplikten etter forskriftens § 7–27 ved behandling av sensitive personopplysninger.

GDPR inneholder flere nye regler om – og for – personvernombud. Den viktigste endringen er at enkelte virksomheter pålegges å ha personvernombud. Dette gjelder alle offentlige virksomheter (med unntak av domstolene), samt alle virksomheter hvis kjerneaktivitet består i regelmessig og systematisk overvåking av personer i stort omfang, eller behandling av sensitive personopplysninger i stort omfang. Etter de nye reglene kreves det ikke lenger at Datatilsynet godkjenner personvernombudet, men det er fortsatt virksomhetens ansvar å utpeke et ombud som oppfyller kravene til personvernombud. Disse kravene er skjerpet i GDPR, blant annet ved at det legges opp til at vedkommende skal «utpekes på grunnlag av faglig egnethet, og i særdeleshet, spesialkunnskaper om personvernrett».

Videre stiller GDPR strengere krav til virksomhetens involvering av personvernombud, og ombudet tillegges flere oppgaver. Personvernombudet skal rapportere til øverste leder, og stillingen er særskilt vernet mot oppsigelser ved konflikt knyttet opp mot personvernspørsmål.

Straffenivået skjerpes kraftig

En annen svært viktig endring i GDPR er nye sanksjonsregler. Hittil har det vært opp til den enkelte medlemsstaten å fastsette sanksjonsnivået for overtredelser av personvernregler, og i Norge kan Datatilsynet etter gjeldende regler ilegge gebyrer på inntil 10G (i dag 925 760 kr).

Ved ikrafttredelsen av GDPR økes bøtenivået betraktelig. For de groveste overtredelsene av de mest sentrale personvernreglene skal det være mulig å ilegge gebyrer på opptil 20 millioner euro eller inntil 4 % av virksomhetens årlige, globale omsetning dersom dette beløpet er høyere. Sammenlignet med dagens nivå i Norge vil altså maksimalt gebyrnivå være *minimum* 180 ganger så høyt – og vesentlig høyere dersom det er snakk om grove overtredelser foretatt av store, globale selskaper.

Når vil de nye reglene gjelde i Norge?

GDPR er endelig vedtatt i EU, og blir automatisk nasjonal lovgivning for EUs medlemsland når de trer i kraft 25. mai 2018. Ettersom GDPR ikke på samme måte blir nasjonal lovgivning i EØS-medlemsland, må Norge i stedet implementere de nye reglene i lovgivningen. De norske reglene som implementerer GDPR, vil imidlertid tre i kraft på samme tid. Virksomheter som ikke har innrettet seg etter reglene etter dette, løper dermed en risiko for å bli ilagt sanksjoner av Datatilsynet.

1 Behandlingsansvarlig er i personopplysningsloven definert som «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes».