

Justis- og beredskapsdepartementet

Sopra Steria AS
Biskop Gunnerus' gate 14A
Postboks 2
N-0051 OSLO
Tlf.: +47 22 57 56 00
Foretaksnummer: NO 910 909 088 mva.
soprasteria.no

Deres ref: 17/4200 ES ØMO/bj Vår ref: PL/H2017/1

16. oktober 17

Høring om utkast til ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett

Sopra Steria AS (Sopra Steria) viser til Justis- og beredskapsdepartementets høring om utkast til ny personopplysningslov for gjennomføring av personvernforordningen i norsk rett med frist 16. oktober 2017.

Sopra Steria ønsker å komme med enkelte innspill til forslaget ettersom selskapet i dag er ett av Norges største konsultentselskaper innenfor fagområder som konsulentrådgivning, programvareutvikling og it-drift. Personvern er et sentralt element i vår hverdag både gjennom rådgivning innenfor informasjonssikkerhet, utvikling og forvaltning av programvare eller drift av it-systemer.

1. Innledning

Fra et overordnet perspektiv forstår Sopra Steria at departementet ikke har store muligheter for nasjonal tilpasning som på noen vesentlig måte kan endre regelverket. Derfor er våre innspill i praksis begrenset. Samtidig innebærer det etter vårt syn at ved implementering av en EU-forordning så øker kravet til veiledning. Våre innspill har derfor større fokus på klargjøring og forståelse enn behovet for endring.

Vi erfarer at det gjennom media og enkelte faggrupper det siste året har blitt fremmet en skremselspropaganda knyttet spesielt til bøtesystemet rundt personvernforordningen. Sopra Steria tror ikke den type skremselspropaganda er heldig, men at den kan avhjelpes ved god veiledning fra relevante myndigheter.

Sopra Steria er en samarbeidspartner for både aktører innenfor offentlig og privat sektor hvor vi bistår med mange aspekter ved digitalisering. Personvern er for vårt vedkommende en iboende del som må hensyntas ved digitaliserings- og automatiseringsprosjekter. Det er derfor også gledelig at personvernforordningen i stor grad viderefører eksisterende regler.

2. Konkrete tilbakemeldinger

a. Personvernombud og personvernrådgiver

Departementet har valgt å benytte begrepet personvernrådgiver i stedet for personvernombud. Sopra Steria er av den oppfatning at begrepet personvernrådgiver ikke treffer den type rolle som søkes løst, og at eksisterende begrep, «personvernombud», i større grad dekker den type uavhengig rolle. Vi ber derfor departementet revurdere begrepet. Det vil da stå mer i samsvar med det svenske og også det engelske begrepet.

En rådgivertittel gir lite veiledning i forhold til hvem som skal rådgis. Det gir heller ingen indikasjon på uavhengighet og forholdet til det som i mange tilfeller er en svakere part, nemlig den registrerte. En rådgiver vil oftest oppfattes som en innleid ressurs som skal ivareta en virksomhets interesser. Et ombud vil derimot oftest oppfattes som en person som har som oppgave å beskytte enkeltpersoners eller grupperes interesser og

rettigheter. Begrepet er godt innarbeidet flere steder i samfunnet, slik som Forbrukerombudet og Sivilombudsmannen, for å verne den enkelte.

Et annet argument for å beholde det eksisterende begrepet er at det til nå har vært en frivillig ordning å oppnevne personvernombud. Ved å beholde eksisterende begrep så understøttes eksisterende frivillige praksis, og begrepet personvernombud gir også større tyngde internt i virksomheter som kan gjøre rekruttering av rollen noe enklere.

b. Veiledning

Sopra Sterias mest sentrale tilbakemelding er likevel knyttet til hvordan departementet kan sikre god og forståelig anvendelse av regelverket. Det er vår oppfatning at eksisterende lovgivning har hatt en stor styrke ved at personopplysningsloven er blitt understøttet av personopplysningsforskriften. I praksis har forskriften gitt aktører god veiledning for å kunne møte lovens krav, slik som innenfor risikoanalyse og informasjonssikkerhet. Ved gjennomføring av personvernforordningen forsvinner forskriften. Selv om dette er nødvendig på grunn av gjennomføringen av forordningen, så oppfordres departementet til å finne gode alternativer til en mer detaljert veiledning enn den som fremkommer av høringen. Det er spesielt viktig at ikke all tolkning og forståelse av forordningen overlates til rettspraksis.

Konkret så ser vi flere områder hvor veiledning vil være sentralt for å sette gode rammer for utøvelse av forordningen:

- Varsling. Det fremkommer en varslingsplikt for virksomheter som behandler personopplysninger når det oppstår brudd på personopplysningsikkerheten senest innen 72 timer. Det fremkommer at denneplikten inntreffer når det er «sannsynlig at bruddet på personopplysningsikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter» (13.6.2 i høringen). Det gir liten veiledning for hvordan dette skal praktiseres.
- Bøter. Under punkt 23.2 redegjøres det for bøtesystemet i forordningen, og at skal legges vekt på «karakteren, alvorlighetsgraden og varigheten av overtredelsen, om overtredelsen er begått forsettlig eller uaktsomt, osv». Det antas at dette skal gi inntrykk av at det må eksistere en proporsjonalitet i bøtesystemet i henhold til EU-retten uten at dette sies. De betraktningene som skal vektlegges er veldig generelle og gir liten veiledning for norske virksomheter når det er aktuelt med en bot tilsvarende «4% av den samlede globale årsomsetningen» til en virksomhet. Vi utfordrer derfor departementet til å være tydeligere for å klargjøre bøtesystemet i forordningen og utnytte bedre mulighetene etter artikkel 84 til fritt å velge hvilke sanksjoner som er passende.
- Portabilitet. En av forordningens nyskapninger er dataportabilitet. Dette er en relativt kjent materie innenfor enkelte områder, slik som portabilitet innenfor telefoni og bank/forsikring. Det som likevel er kjennetegnet for områder hvor det finnes portabilitet er at det er etablert standarder for hva som er nødvendig å avgi av informasjon til en annen for å sikre en sømløs overføring av tjenester. Foreslåtte regler om dataportabilitet er derimot generelle og angir liten veiledning for hvordan dataportering skal gjennomføres i praksis (dog vises det til Artikkel 29-gruppens veiledning). Det kan eksempelvis være normer for portering eller ansvar mellom avgivende og mottakende. Når det gjelder ansvar for portering kan nevnes eksempelvis når avgivendes ansvar opphører og data kan slettes.

Med vennlig hilsen



Peter Lenda

Director Legal and Compliance
Sopra Steria Scandinavia