SKAL - ELLER BØR - I UDPEGE EN DATA PROTECTION OFFICER?

I sidste nummer af Ret & Indsigt bragte vi en artikel om den nye rolle som databeskyttelsesrådgiver (DPO). Her beskrev vi bl.a., at der var nogen usikkerhed forbundet med fortolkningen af databeskyttelsesforordningens regler om udpegning af DPO'er og DPO'ers nærmere forpligtelser og ansvar.

Nu har den såkaldte Artikel 29-gruppe offentliggjort retningslinjer samt Q&A's, der bringer noget mere klarhed vedrørende disse spørgsmål. Det beskriver vi i denne artikel med fokus på, hvem der skal og bør udpege en DPO.

HVEM SKAL OG BØR UDPEGE EN DPO?

Ifølge forordningens artikel 37, stk. 1, skal der udpeges en DPO, når:

- behandlingen af persondata foretages af en offentlig myndighed eller et offentligt organ
- kerneaktiviteterne i den relevante virksomhed består af behandlingsaktiviteter, der kræver regelmæssig og systematisk overvågning af individer i stort omfang, eller
- kerneaktiviteterne i den relevante virksomhed indebærer behandling af særligt følsomme oplysninger, herunder vedrørende straffedomme og lovovertrædelser i stort omfang.

Offentlige myndigheder og organer

Det fremgår af vejledningen, at begrebet "offentligt organ" skal fortolkes efter national lovgivning.

I dansk ret har vi ikke en fast definition af begrebet "offentligt organ", hvorfor der er usikkerhed forbundet med, hvem der er omfattet af dette begreb.

Da kommunale § 60-fællesskaber anses som offentlige myndigheder, er det givet, at de skal udpege en DPO. Kommunalt ejede aktieselskaber, der udfører almennyttige opgaver, vil formentlig anses som et offentligt organ. Derimod er det mere tvivlsomt, om offentlig-private selskaber, der udfører opgaver efter lov 548 som f.eks. vej- og parkopgaver, skal anses som et offentligt organ.

Der er ikke direkte i forordningen eller vejledningen taget stilling til, om offentlige myndigheder og organer, der foretager udbud af deres opgaver, f.eks. af plejehjemsdrift, eller på anden måde overlader behandling af personoplysninger til databehandlere, skal stille som krav, at den vindende tilbudsgiver/databehandler har en DPO i forhold til oplysninger knyttet til de udbudte opgaver. Ud fra omgåelsesbetragtninger synes meget at tale for, at dette burde være tilfældet. Det fremgår imidlertid af vejledningen, at selvom en dataansvarlig er forpligtet til at udpege en DPO, gælder dette ikke nødvendigvis for den dataansvarliges databehandlere. Det anføres dog, at det vil være god praksis at gøre det.

Forsyningssektoren mv.

Artikel 29-gruppen anbefaler tillige, at organisationer, der er reguleret af offentlige og privatretlige regler, og som udfører "offentlige opgaver" inden for offentlig transport, vand- og energiforsyning, offentlig infrastruktur, public service radio samt tv og offentlige boliger, også udpeger en DPO, selvom de ikke er forpligtede hertil. Tillige er det anbefalingen, at DPO'en fører tilsyn med alle de behandlinger, der udføres – også dem, der ikke relaterer sig til udførelsen af den offentlige rolle (eksempelvis behandlingen i en medarbejderdatabase).

Baggrunden for anbefalingen er, at de registrerede – som når offentlige myndigheder eller offentlige organer behandler personoplysninger – ofte ikke har noget eller kun begrænset valg i forhold til behandlingen af deres data. Det medfører et behov for den yderligere beskyttelse, som udpegningen af en DPO kan give.

Private virksomheder

Om en privat virksomhed eller organisation skal udpege en DPO beror på, om virksomhedens behandlingsaktiviteter opfylder kriterierne i forordningens artikel 37.

Vejledningen gør det klart, at "kerne-aktivitet" skal forstås som de centrale behandlinger, en virksomhed udfører for at forfølge sine overordnede formål, og som dermed uløseligt er forbundet hermed. Eksempelvis anses et hospitals behandling af helbredsoplysninger som nødvendig for at forfølge hospitalets vigtigste mål. Endvidere vil private sikkerhedsfirmaer, der udøver overvågning af en række private shoppingcentre, uundgåeligt komme til at behandle personoplysninger, hvilket derfor må anses som en kerneaktivitet for sådanne virksomheder. Disse skal derfor udpege en DPO.

Derimod vil virksomheders behandling af personoplysninger i forbindelse med almindelige lønningslister og interne it-tjenester sædvanligvis blive anset for biaktiviteter. Ifølge Artikel 29-gruppens vejledning medfører det ikke i sig selv en forpligtelse til at udpege en DPO.

"Stort omfang" bestemmes ud fra bl.a. mængden af data, mængden af registrerede personer samt den tidsmæssige udstrækning af behandlingen. Eksempler på "stort omfang" er:

- rejsedata for personer, der anvender et offentligt transportsystem (f.eks. ved brug af periodekort/rejsekort)
- kundedata som led i den normale drift af et forsikringsselskab eller en bank
- data i forbindelse med adfærdsbaseret markedsføring af en søgemaskine
- indholds-, trafik- og lokationsdata af telefonselskaber eller internetudbydere.

Ifølge vejledningen skal begreberne "regelmæssig og systematisk overvågning af registrerede" forstås som en aktivitet, der gentages med en vis frekvens og er planlagt, eller strategisk, dvs. mere end en tilfældighed. Det kan f.eks. være sporing og profilering på internettet ved brug af cookies til adfærdsbaseret markedsføring, herunder sporing af placering via mobile apps, loyalitetsprogrammer eller elektroniske enheder, der kan skabe forbindelse til f.eks. smartbiler, intelligente målere mv.

HVAD ER EN DPO?

En DPO er en person – enten en medarbejder eller en ekstern konsulent – som underretter, informerer og rådgiver sin opdragsgiver om regler og retningslinjer for at overholde krav til databeskyttelse.

DPO'en kan være fælles for flere myndigheder eller offentlige organer, men det understreges i vejledningen, at DPO'en ikke må have større arbejdsbyrde, end at vedkommende effektivt kan udføre sine opgaver.

KRAV TIL DPO'EN

En DPO skal have passende faglige kvalifikationer og ekspertviden om databeskyttelseslovgivningen nationalt og i EU for at kunne udfylde sin rolle. Vejledningen angiver, at kravet til niveauet af ekspertise må afhænge af behandlingsaktiviteterne – jo mere komplekse eller risikofyldte behandlingsaktiviteterne er, jo større ekspertise kræves af DPO'en.

Endvidere anføres det, at DPO'en bør have en forståelse for de behandlinger, der sker i myndigheden eller virksomheden.

DPO'er for offentlige myndigheder og organer bør også have en god indsigt i forvaltningsretlige regler og myndighedens organisation.

DPO'ENS UAFHÆNGIGHED

Det er væsentligt, at DPO'en kan udøve sit hverv på uafhængig vis, uanset om denne er ansat hos den dataansvarlige eller ej.

En DPO skal være selvstyrende og uafhængig og må ikke underlægges instrukser fra myndigheden eller virksomheden i forhold til at udføre sine opgaver, f.eks. hvordan eller hvornår denne skal håndtere en specifik opgave.

DPO'en er ikke afskåret fra at udføre andre opgaver og funktioner i en organisation ved siden af sit virke som DPO, men kun sådanne som ikke medfører nogen form for interessekonflikt. Ifølge vejledningen er en tommelfingerregel, at varetagelsen af opgaver i de mest ledende stillinger i en virksomhed formentlig er i konflikt med de opgaver, som DPO'en har. Det er eksempelvis sandsynligt, at en it-chefs opgaver vil være i konflikt med DPO'ens rolle.

USIKKERHED OM, HVEM DER SKAL UDPEGE EN DPO

Som det fremgår ovenfor, bringer vejledningen ikke fuldstændig klarhed over, hvilke offentlige og private organisationer der skal udpege en DPO. Hvis en organisation ikke mener sig forpligtet til at udpege en DPO, anbefales det i vejledningen, at der under alle omstændigheder udarbejdes en intern analyse af, om der skal udpeges en DPO for at demonstrere, at de ovennævnte faktorer er blevet vurderet.

Hertil kommer, at der skal udvises omhu ved udpegningen af en DPO, således at det sikres, at DPO'en har de rette kvalifikationer, og at der ikke er eller opstår interessekonflikter, ligesom det skal afklares, hvor vedkommende organisatorisk skal placeres i organisationen.

Og først når ovennævnte er på plads, kan DPO'en koncentrere sig om de mange opgaver, som en DPO har ■

Mads Nygaard Madsen
Advokat, partner
mnm@horten.dk

Charlotte Kunckel
Specialistadvokat
cku@horten.dk

Diana Sofia Manrique de Lara
Advokatfuldmægtig
dml@horten.dk