2017-09-11

Dataskyddsombud

Krav enligt art. 37 (1) dataskyddsförordningen

Dataskyddsförordningen (GDPR) kommer att gälla som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen kommer att ersätta personuppgiftslagen (1998:204), PuL, och vara direkt tillämplig i Sverige. Dataskyddsförordningen gäller alla som behandlar personuppgifter i sin verksamhet, oavsett om det är en statlig eller privat aktör oaktat organisationens storlek.

Ett nytt krav som införts i dataskyddsförordningen är skyldigheten för myndigheter som behandlar personuppgifter att utse en s.k. Data Protection Officer (DPO), nedan kallad dataskyddsombud. Detta underlag syftar till att redogöra för de krav som lagen ställer på dataskyddsombudets funktion.

Allmänt

Enligt artikel 37 (1) i dataskyddsförordningen är det obligatoriskt att inrätta ett dataskyddsombud om behandlingen sker av myndigheter eller offentligt organ (oavsett vilken data som behandlas). Artikel 29-gruppen har uttalat följande om definitionen av myndigheter och offentligt organ:

- Definitionen ska fastställas genom nationell lagstiftning. Vanligtvis gäller detta myndigheter men andra organ kan även omfattas.
- Liknande verksamheter kan vara uppgifter som sker för landets infrastruktur, public service, vatten och elförsörjning etc. där den registrerade har en begränsad rätt att kontrollera eller bestämma över behandlingen.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

Artikel 29-gruppen rekommenderar att även privata aktörer som utför tjänster i allmänhetens intresse ska utse ett dataskyddsombud.

Dataskyddsombudet är inte personligt ansvarig för det fall myndigheten inte uppfyller kraven enligt dataskyddsförordningen, utan det är alltid personuppgiftsansvariges eller personuppgiftsbiträdes ansvar att se till att all personuppgiftsbehandling sker i enlighet med dataskyddsförordningen (art 24 (1)).

Beroende på hur situationen ser ut kan såväl personuppgiftsansvarig som personuppgiftsbiträdet behöva utse ett dataskyddsombud. Artikel 29-gruppen rekommenderar att personuppgiftsbiträden inrättar dataskyddsombud som god praxis, oavsett om åtagandet är uppfyllt av den personuppgiftsansvarige.

Ett eller flera dataskyddsombud?

Artikel 37 (2) i dataskyddsförordningen möjliggör för ett dataskyddsombud att verka i flera organisationer om denne finns lättillgänglig för samtliga verksamheter. Exempelvis får en koncern utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå dataskyddsombudet.

Dataskyddsombudet ska ge ut kontaktuppgifter i enlighet med förordningen och ska effektivt kunna kommunicera med registrerade och tillsynsmyndigheten.

När den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.

Beroende på organisationens storlek kan det behövas ett team bestående av flera dataskyddsombud. I sådant fall ska samtliga medlemmars roller och ansvar specificeras.

Vid bedömning om huruvida ett dataskyddsombud kan vara verksam inom flera verksamheter bör hänsyn tas till storleken på verksamheten samt den organisatoriska strukturen.

Vem bör utses som dataskyddsombud?

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal. Dataskyddsombudet kan således utföra andra uppgifter eller uppdrag. Personuppgiftsansvarige eller personuppgiftsbiträdet ska dock se till att sådana uppgifter eller uppdrag inte leder till en intressekonflikt. Artikel 29-gruppen har angett ett flertal exempel på roller där en intressekonflikt med dataskyddsombudet skulle kunna föreligga, bland annat vd, operativ chef, ekonomichef, marknadschef, HR-chef samt it-chef.

Enligt artikel 29-gruppen bör personuppgiftsansvarige och personuppgiftsbiträde identifiera roller som kan stå i konflikt med dataskyddsombudets roll samt upprätta interna regler om intressekonflikter. Vidare bör det inom organisationen dokumenteras att det inte föreligger några intressekonflikter. Avtal som upprättas bör vara tillräckligt detaljerade.

Dataskyddsombudets roll

Dataskyddsombudets uppgift är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser. Dataskyddsombudet ska även vara en kontaktpunkt för tillsynsmyndigheten och de registrerade.

Det är viktigt att dataskyddsombudets arbete utförs med tillräcklig självständighet och att ombudet rapporterar direkt till högsta ledningen. Personuppgiftsansvarige eller personuppgiftsbiträde får inte ge instruktioner om hur arbetet ska utföras. Detta innebär emellertid inte att dataskyddsombudet har någon beslutande rätt. Det är fortfarande personuppgiftsansvarige eller personuppgiftsansvarige som har det yttersta ansvaret för att dataskyddsförordningen följs.

Personuppgiftsansvarige och personuppgiftsbiträde ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter och se till att dataskyddsombudet involveras i ett tidigt skede gällande alla frågor som rör dataskydd.

Personuppgiftsansvarige och personuppgiftsbiträde ska rådgöra med, och informera, dataskyddsombudet om alla åtgärder som kan komma att påverka efterlevnad av dataskyddsförordningen. Att rådgöra med dataskyddsombudet bör inrättas som en standardprocedur inom organisationen.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

Vidare ska organisationen säkerställa att:

- dataskyddsombudet blir inbjudet till att regelbundet delta i ledningsgruppens möten,
- dataskyddsombudet närvarar på möten som rör frågor om dataskydd,
- dataskyddsombudets åsikt ges betydelse,
- dataskyddsombudet omgående blir informerad om överträdelser av lagen eller när en personuppgiftsincident upptäcks,
- dataskyddsombudet får, när lämpligt, ge synpunkter på de riktlinjer för dataskydd som personuppgiftsansvarige och personuppgiftsbiträde tar fram.

Personuppgiftsansvarige och personuppgiftsbiträde ska stödja dataskyddsombudet i utförandet av dennes uppgifter genom att tillhandahålla de resurser som krävs för att dataskyddsombudet ska kunna fullgöra sina uppgifter.

Det är viktigt att dataskyddsombudets roll och uppgifter kommuniceras internt till samtliga medarbetare. Personuppgiftsansvarige ska se till att dataskyddsombudet får tillgång till funktioner som HR, juridik, it, säkerhet m.m. när så behövs samt att dataskyddsombudet får tillräckligt stöd i form av finansiella resurser, kommunikation samt personal. Dataskyddsombudet ska få tillräckligt med stöd från ledningen samt tillräckligt med tid för att kunna fullgöra sina uppgifter. Som huvudregel kan nämnas att ju mer komplex och/eller känslig personuppgiftsbehandlingen är desto mer resurser måste dataskyddsombudet få.

Dataskyddsombudet ska få regelbunden utbildning i frågor som rör dataskyddsförordningen.

Anställda ska kunna rapportera iakttagelser eller incidenter till dataskyddsombudet. Därför omfattas dataskyddsombudet av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL.

Dataskyddsombudet får inte bli föremål för sanktioner av personuppgiftsansvarige för att ha utfört sina uppgifter enligt lagen.

Dataskyddsombudets expertis och meriter

- Enligt art. 37(5) ska dataskyddsombudet utses på grundval av yrkesmässiga kvalifikationer, och i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39 och skäl 97.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

- Expertisnivån måste vara proportionell till komplexiteten, känsligheten och mängden av data som organisationen behandlar. Ju mer komplex och känslig data som behandlas desto högre nivå av expertis och stöd krävs.
- Dataskyddsombudet ska ha kunskap om nationella och europeiska dataskyddslagar och praxis samt ha en djup förståelse för dataskyddsförordningen.
- Dataskyddsombudet bör ha kunskap om organisationens verksamhetsområde och bransch.
- Dataskyddsombudet bör även ha en bra förståelse för de behandlingar som utförs, informationssystemen, informationssäkerheten och dataskydd samt personuppgiftsansvariges behov.
- När det gäller myndighet bör dataskyddsombudet även ha god kunskap om myndighetens administrativa regler och processer.
- Dataskyddsombudet ska ha en förmåga att fullfölja sina uppgifter med hög integritet och professionell etik.

Mer information om dataskyddsombud finns under följande webbplatser;

SKL -
https://skl.se/download/18.2ced2eb215cc46662ca11a3a/1498030987866/V%C3%A4gledning%20kring%20dataskyddsombud.pdf

Datainspektionen -
http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/dataskyddsombud/

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se