10.

STOHAB
2018-05-22

Till Stockholms Hamn AB:s styrelse

Utseende av dataskyddsombud för Stockholms Hamn AB

Bakgrund

Den 25 maj 2018 träder den nya dataskyddsförordningen i kraft (GDPR; General Data Protection Regulation), nedan kallad Förordningen. Förordningen ska tillämpas av alla som behandlar personuppgifter i sin verksamhet inom såväl offentlig som privat sektor och oavsett organisationens storlek. Förordningen ersätter personuppgiftsdirektivet från 1995 och personuppgiftslagen (PuL).

Det övergripande syftet med Förordningen är att skydda enskildas grundläggande rättigheter och friheter och då särskilt deras rätt till skydd av personuppgifter och därmed även rätten till skydd för privatlivet. Ett annat syfte är att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU vilket uppnås genom att Förordningen är direkt tillämplig i alla medlemsstater. Syften har även varit att dataskyddsdirektivet från 1995, vilket är det som PuL bygger på, behövde moderniseras för att anpassas till det nya digitala samhället.

Mycket av det som Förordningen reglerar gäller redan i dag genom PuL men den personuppgiftsansvarige får en del nya uppgifter och skyldigheter och de registrerade får nya och utökade rättigheter.

Förordningen innebär bland annat följande förändringar:

1. Ökade krav på hantering av personuppgifter

Förordningen innebär att den s.k. missbruksregeln inte längre finns kvar. Det handlar t.ex. om information om personer i e-post, på internet eller i en enkel lista som finns i datorn. När missbruksregeln nu försvinner så innebär det att samma regler kommer att gälla för all hantering av personuppgifter, även i e-post och på webbplatser.

2. Ökade krav på information till den registrerade

Varje bolag inom koncernen Stockholms Stadshus AB är personuppgiftsansvarigt för de uppgifter som bolaget behandlar i sin verksamhet och ansvarar således också för en korrekt personuppgiftshantering. Den enskilda individen får genom Förordningen stärkt makt över sina personuppgifter genom rätten till insyn, till rättelse och radering. Den verksamhet som behandlar/registrerar en personuppgift måste informera den registrerade om varför (på vilken laglig grund) och hur länge informationen sparas. Det är inte heller tillåtet att samla in och behandla fler uppgifter än vad som är nödvändigt för ändamålet.

3. Krav på incidentrapportering inom 72 timmar

För det fall en incident inträffar, exempelvis att ett register kommer i orätta händer eller uppgifter skickas till fel mottagare, måste de finnas beredskap för att upptäcka, rapportera och utreda sådana incidenter. En personuppgiftsincident ska rapporteras till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den.

4. Sanktionsavgifter införs

För det fall en överträdelse konstateras kan en sanktionsavgift motsvarande 10-20 miljoner euro eller 2-4 % av organisationens globala årsomsättning utgå. För myndigheter föreslås en motsvarande sanktionsavgift om upp till 10 miljoner kronor.

5. Dataskyddsombud

Enligt Förordningen är det obligatoriskt för vissa personuppgiftsansvariga att utse ett dataskyddsombud. Så kommer att vara fallet för alla offentliga myndigheter och organ och för andra organisationer som har som sin kärnverksamhet att systematiskt och i stor omfattning övervaka enskilda personer eller behandla särskilda kategorier av personuppgifter i stor omfattning. Även om Förordningen inte innehåller ett specifikt krav på att utse ett dataskyddsombud kan det ibland vara bra att göra det frivilligt.

Dataskyddsombud

Dataskyddsombud är ingen ny företeelse och även om det gamla dataskyddsdirektivet inte föreskriver ett särskilt utnämnande av dataskyddsombud har många medlemsstater utvecklat en praxis för att göra detta. Dataskyddsombudet är dock inte personligen ansvarigt för det fall organisationen brister i sin efterlevnad. Det ansvaret ligger alltid på den personuppgiftsansvariga, det vill säga den juridiska personen (bolaget).

Dataskyddsombudets uppgifter

Dataskyddsombudets uppgift är enligt artikel 39 att informera och ge råd till den personuppgiftsansvarige om skyldigheterna enligt förordningen, samt att övervaka den personuppgiftsansvariges efterlevnad av förordningen. Ombudets uppgift är även att samla in information om hur verksamheten behandlar personuppgifter.
Dataskyddsombudet ska vidare delta i de konsekvensbedömningar som ska genomföras, samarbeta med tillsynsmyndigheten (Datainspektionen) och utgöra kontaktpunkt för såväl tillsynsmyndigheten som de registrerade.

Dataskyddsombudets ställning

Dataskyddsombudet ska enligt artikel 38 delta i alla frågor som rör skyddet av personuppgifter, rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå och ha de resurser som krävs för att fullgöra sina uppgifter. Ombudet får inte ta emot några instruktioner från den personuppgiftsansvarige vad gäller hur ombudets uppgifter ska utföras och får heller inte avsättas eller utsättas för sanktioner för att ha utfört sina uppgifter.

Dataskyddsombudets kompetens

I artikel 37.5 föreskrivs vissa yrkesmässiga kvalifikationer som gäller för ett dataskyddsombud exempelvis

- Kunskap om dataskyddslagstiftning och praxis på nationell nivå och EU-nivå, inklusive djupgående kunskap om den allmänna dataskyddsförordningen.
- Förståelse av hur behandlingen av personuppgifter genomförs.
- Kunskap om olika typer av informationsteknik och datasäkerhet.
- Kunskap om affärssektorn och organisationen i fråga.
- Förmåga att främja en dataskyddskultur inom organisationen.

Dataskyddsombudets roll

Enligt artikel 37.6 får dataskyddsombudet ingå i den personuppgiftsansvariges personal eller utföra uppgifterna på grundval av ett tjänsteavtal. Det är enligt artikel 37.2 även möjligt för en koncern att utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.

Ett dataskyddsombud får enligt artikel 38.6 fullgöra andra uppgifter och uppdrag än de som följer av förordningen. Dessa uppgifter får dock inte leda till en intressekonflikt. Det innebär att dataskyddsombudet inte kan inneha en sådan tjänst inom organisationen som innebär att denne fastställer ändamålen med och medlen för behandlingen av personuppgifter. Sådana motstridiga befattningar inom organisationen kan exempelvis vara befattningar i högsta ledningen (t.ex. verkställande direktör eller IT-chef).

Sammanfattande bedömning

Stockholms Hamn AB faller inte uppenbart in i det obligatoriska kravet på att utse ett dataskyddsombud. Oaktat detta bör dock ett dataskyddsombud utses.

Stockholms Hamn AB har bedömt att erforderlig kompetens för att tillsätta ett dataskyddsombud finns i bolaget och det innebär att tjänsten inte måste rekryteras externt.

Förordningen medger att en koncern och en myndighet eller ett offentligt organ får utnämna ett enda dataskyddsombud. Mot bakgrund av detta vore det mest ändamålsenliga och effektiva alternativet att ha samma ombud i Stockholms Hamn AB, Kapellskärs Hamn AB och Nynäshamns Mark AB. Tjänsten uppskattas inledningsvis kräva en halvtidstjänst.

Förslag

Styrelsen föreslås besluta

att utse Angelica Wagneryd, Informationssäkerhetssamordnare, till dataskyddsombud i Stockholms Hamn AB.

Stockholm den 7 maj 2018

Johan Castwall
VD