Datainspektionen informerar

Nr 3/2017

Allmänna Råd

Den nya EU-förordningen om dataskydd som träder ikraft i maj 2018 innehåller bestämmelser om ***dataskyddsombudet***. Bestämmelserna reglerar vilken roll och vilka uppgifter dataskyddsombudet ska ha.

Det är obligatoriskt för många organisationer att utse dataskyddsombud, bland annat för myndigheter.

Vägledningen ska tjäna som hjälpmedel vid tillsättande av dataskyddsombud.

Vägledningen grundar sig på EU-förordningens artiklar 37, 38 och 39 samt Artikel 29-gruppens rekommendation.

Datainspektionen

den 29 september 2017

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Innehåll

1 Allmänt

Europaparlamentets och Rådets *förordning* (GDPR) (EU 2016/679) om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om *upphävande av direktiv* 95/46/EC träder i kraft den 25 Maj 2018.

Förordningen fokuserar på personuppgiftsansvarigs[1] ansvar, det vill säga roller, riskbaserat betraktelsesätt, inbyggt dataskydd och dataskydd som standard, register över behandling av personuppgifter, konsekvensbedömning gällande dataskydd och skyldighet att informera om dataintrång.

Förordningen gäller direkt som lag och ersätter nationella regler såsom landskapslag (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen samt landskapslag (2007:89) om Datainspektionen. Förordningen ger utrymme för mer preciserade bestämmelser i nationell lagstiftning (tillsynsmyndighet, personuppgiftsbehandling inom myndigheter, sanktionsavgiften inom offentlig sektor). I dagsläget pågår ännu beredningen av lagstiftningen.

Europeiska dataskyddsstyrelsen (EDPB)[2] ger enligt artikel 68 utlåtanden, rekommendationer och riktlinjer antingen på eget initiativ eller på kommissionens begäran. Därtill ger EDPB rättsligt bindande avgöranden i fall där nationell myndighet har avvikande tolkning.

Förordningen innehåller uttryckliga krav på att stöd och resurser används inom organisationen, att dataskyddsombudet ska rapportera till högsta ledningen och inte får utsättas för repressalier.

Uppgift om dataskyddsombud ska anmälas till Datainspektionen.

Datainspektionen ger vägledning till dataskyddsombuden. På webbplatsen www.di.ax finns informationsmaterial om lagstiftningen och dess tillämpning.

2 Vad är ett dataskyddsombud?

Myndigheter eller annat offentligt organ ska under alla omständigheter utse en person i organisationen alternativt anställa eller genom uppdragsavtal ge en annan organisation i uppdrag att bevaka dataskyddet. Det gäller även för organisationer som hanterar känsliga

[1] *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

[2] Innan förordningen trätt i kraft tar Artikel 29-gruppen ställning i dessa frågor.

uppgifter[3] i stor skala. Även kommersiella aktörer som utför myndigheters hantering av personuppgifter ska utse dataskyddsombud[4]. Dataskyddsförordningen (GDPR) definierar inte vad som avses med offentlig myndighet eller offentligt organ. Således är det upp till varje medlemsland att i den nationella lagstiftningen definiera vad som avses. Ännu idag är det inte klart hur begreppet kommer att definieras i åländsk lagstiftning.

Ett dataskyddsombud ser till att personuppgifter behandlas på ett korrekt och lagligt sätt inom den egna organisationen. Rollen regleras utförligt i förordningen.

2.1 Behörighetskrav

Lagstiftningen ställer ingen specifikation på utbildnings- eller certifieringskrav på dataskyddsombudet. Däremot ställs tydliga krav på kompetens och lämplighet för att kunna handha de uppgifter verksamheten förutsätter.

Dataskyddsombudet ska, enligt artikel 37.5, utses på grundval av yrkesmässiga kvalifikationer och sakkunskap om lagstiftning och praxis avseende dataskydd. Det är önskvärt att dataskyddsombudet väljs med stor omsorg. Enligt vägledningen om dataskyddsombud från den 13 december 2016[5] ska dataskyddsombudet ha:

- Expertkunskaper beträffande nationella och europeiska dataskyddsbestämmelser och dataskyddspraxis samt djupa kunskaper beträffande EU:s dataskyddsförordning,
- Kännedom om myndighetens organisation,
- Tillräckliga kunskaper om databehandlingen som myndigheten utför samt IT-systemet, datasäkerheten och dataskyddet som myndigheten behöver,
- Gedigna kunskaper om regelverket som tillämpas i myndighetens verksamhet samt
- Integritet och högstående yrkesetik

Nivån på kunskap bestäms på basis av vilken typ av databehandling och vilken typ av känslighet uppgifterna har. I de fall databehandlingen till exempel är speciellt komplex eller en stor mängd känsliga personuppgifter behandlas ställs krav på en högre nivå på kunskap och stöd.

2.2 Hur ska kontaktuppgifterna till dataskyddsombudet tillkännages?

Den personuppgiftsansvariga organisationen ska offentliggöra dataskyddsombudets kontaktuppgifter. Avsikten är att försäkra sig om att de registrerade, både anställda, kunder och

[3] Kärnverksamheten består av behandling, som på grund av sin karaktär, omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning eller består av känsliga personuppgifter eller som rör fällande domar i brottmål och överträdelser.
[4] Enligt Artikel 29-gruppens ställningstagande 13.12.2016.
[5] Här avses Artikel 29-gruppen http://ec.europa.eu/justice/data-protection/index eu.htm

andra, på ett enkelt sätt kan kontakta ombudet utan att först ta kontakt med en annan del av organisationen.

Kontaktuppgifterna bör bestå av sådan information som på ett enkelt sätt möjliggör för de registrerade och Datainspektionen att kontakta dataskyddsombudet (till exempel telefonnummer och/eller e-postadress direkt till ombudet, kontaktuppgifter på webbsidan eller en ”hot-line”, samt postadress).

Organisationen ska också meddela kontaktuppgifterna till Datainspektionen. Datainspektionen kommer inledningsvis att upprätta ett register över kontaktuppgifter. På sikt kommer Datainspektionen att tillhandahålla en registerlösning där den registeransvariga organisationen registrerar kontaktuppgifterna till ombudet.

2.3 Gemensamt ombud

Flera myndigheter kan i enlighet med artikel 37.3 ha ett dataskyddsombud tillsammans, om det är lämpligt med hänsyn till deras organisationsstruktur och storlek. Vid bedömningen av hur stort arbetsområde ett och samma dataskyddsombud kan ha gäller det dock att beakta att arbetsbördan inte får bli oskäligt stor och att det inte får bli orealistiskt svårt för dataskyddsombudet att förvärva tillräcklig kännedom om alla de berörda myndigheternas behandling av personuppgifter och om alla författningar som inverkar på den aktuella hanteringen av personuppgifter.

Det är möjligt att antingen ha ett anställt dataskyddsombud eller att anlita ett dataskyddsombud genom ett uppdragsavtal (artikel 37.6).

2.4 Uppgifter

Till uppgifterna för en myndighets dataskyddsombud hör bland annat att ge råd och information inom myndigheten angående de gällande dataskyddsbestämmelserna, att övervaka efterlevnaden av dataskyddsförordningen, andra dataskyddsbestämmelser samt myndighetens strategi för skydd av personuppgifter och att samarbeta med Datainspektionen (artikel 39). Enligt artikel 35:2 ska myndigheten rådfråga sitt dataskyddsombud vid genomförande av konsekvensbedömningar för databehandling som sannolikt leder till hög risk för människors rättigheter och friheter.

Personer, vars personuppgifter registrerats, har enligt artikel 38.4 rätt att kontakta dataskyddsombudet angående alla frågor som rör behandlingen av deras personuppgifter och utövandet av deras rättigheter enligt dataskyddsförordningen.

I enlighet med artikel 38.1-3 ska myndigheten

- säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter,
- stödja dataskyddsombudet i hans eller hennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra uppgifterna, genom att ge tillgång till personuppgifter och behandlingsförfaranden samt genom att upprätthålla dataskyddsombudets sakkunskap,
- säkerställa att dataskyddsombudet inte tar emot instruktioner från utomstående personer beträffande utförandet av sina uppgifter,
- avhålla sig från att säga upp eller avskeda dataskyddsombudet eller att på annat sätt bestraffa dataskyddsombudet för att han eller hon har utfört sina uppgifter
- samt låta dataskyddsombudet rapportera direkt till myndighetens högsta förvaltningsnivå.

Dataskyddsombudet får fullgöra även andra uppgifter och uppdrag, utöver sin uppgift som dataskyddsombud, men de andra uppgifterna och uppdragen får inte medföra att dataskydds-ombudet hamnar i en intressekonflikt (artikel 38.6).

Dataskyddsombuden har en mycket viktig funktion. Det är nödvändigt att se till att de har tillräcklig tid avsatt för att utföra sina uppdrag på ett bra sätt.

2.5 Dataskyddsombudets ställning

Den personuppgiftsansvarige och personuppgiftsbiträdet[6] ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Vidare ska den personuppgiftsansvarige och personuppgiftsbiträdet stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap. För att dataskyddsombudet ska få tillräcklig information och bli tillräckligt involverad i alla processer rekommenderar Datainspektionen att verksamheten garanterar att:

1. Dataskyddsombudet regelbundet deltar i möten på högsta ledningsnivå och mellanchefsnivå
2. Dataskyddsombudet är närvarande och får yttra sig över beslut som har eventuella dataskyddskonsekvenser
3. Dataskyddsombudets bedömning efterfrågas och tas till vara. Vid oenighet kan det vara bra att dokumentera varför dataskyddsombudets bedömning inte följs

[6] *Personuppgiftsbiträde:* en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

4. Dataskyddsombudet informeras när väsentliga rutiner ändras eller nya IT-system och säkerhetsåtgärder ska utvecklas
5. Dataskyddsombudet informeras och tillfrågas om råd vid avvikelser från dataskydds-lagstiftningen eller andra händelser som kan ha konsekvenser för dataskyddet.

Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

2.6 Anmäla eller avanmäla dataskyddsombud

Anmälan eller avanmälan av dataskyddsombud kan göras genom att använda en särskild anmälningsblankett som kommer att finnas på www.di.ax