Datainspektionens granskning av utnämningen av dataskyddsombud 2019

Datainspektionen inledde den 18 mars 2019 en granskning av Ålands landskaps och kommunala myndigheters utnämnande av dataskyddsombud.

Detta är den första övergripande granskningen Datainspektionen gjort sedan dataskyddsförordningens ikraftträdande 25 maj 2018.

Följande är en rapport över granskningen.

Datainspektionen

den 12 december 2019

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

1 Lagstöd och anledningen till granskningen

1.1 Anledning till granskningen

Den 8 maj 2018 beslutadesamtliga nordiska dataskyddsmyndigheter förutom Färöarna att granska huruvida organisationer som har en lagstadgad skyldighet att ha ett dataskyddsombud även anlitat detsamma. Åland var med och undertecknade dokumentet där detta framgår, den så kallade Köpenhamnsdeklarationen.

Någon granskning av utnämnande av dataskyddsombud gjordes dock inte under 2018. I samband med att den nya myndighetschefen tillträdde i tjänst den 1 mars 2019 beslutades därför att granskningen skulle inledas så snart som möjligt. Granskningen inleddes formellt den 18 mars 2019.S

1.2 Lagstöd

Enligt Europaparlamentets och Rådets Förordning (EU) 2016/679 av den 27 april 2016 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/EG (den allmänna dataskyddsförordningen) artikel 37 ska ”[d]en personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om behandlingen genomförs av en myndighet eller ett offentligt organ”.

Av samma artikel framgår även att ”[o]m 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”.

Sammantaget innebär detta att samtliga myndigheter och offentliga organ inom Ålands landskaps och kommunalförvaltning måste utnämna dataskyddsombud, men det finns inget hinder mot att de olika myndigheterna eller organen använder samma person, så länge det är en lämplig lösning.

Att Datainspektionen har rätt att utföra granskningar av denna typ framgår av Dataskyddsförordningens artikel 57: ”Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för [att] [...] övervaka och verkställa tillämpningen av denna förordning”. Det framgår vidare i artikel 58 att Datainspektionen har befogenhet att begära information från sina tillsynsobjekt, genomföra undersökningar i form av dataskyddstillsyn, utfärda varningar, reprimander, förelägganden och införa begränsningar i behandling, bland annat.

2 Granskningen

2.1 Metod

Granskningen inleddes genom att de dataskyddsombud som registrerats hos Datainspektionen kontaktades för att bekräfta deras ställning som dataskyddsombud. Dataskyddsombuden ombads därför via e-post att skicka de beslut eller avtal som utgjorde grunden för deras utnämnande. Dataskyddsombuden vidarebefordrade denna begäran till sina huvudmän. De tillsynsobjekt som utnämnt dataskyddsombud delgav i samband med detta Datainspektionen om detta, de tillsynsobjekt som inte utnämnt dataskyddsombud skickades en rekommendation att utnämna dataskyddsombud. En kommun motsatte sig Datainspektionens tolkning av lagstiftningen, denna

kommuns personuppgiftsansvariga organ blev därmed föremål för ett föreläggande att utnämna dataskyddsombud. Inget av de personuppgiftsansvariga organen besvärade sig mot föreläggandet.

Tillsynsobjekten kan delas in i fem olika kategorier:

1. De som anlitat dataskyddsombud internt,
2. De som anlitat dataskyddsombud externt,
3. De som anlitat dataskyddsombud redan innan granskningen inleddes,
4. De som anlitat dataskyddsombud efter att granskningen inleddes,
5. De som ännu ej anlitat dataskyddsombud.

Totalt har 102 organ varit föremål för granskning. Tio av dessa är myndigheter inom landskapsförvaltningen underställda landskapsregeringen, sex är kommunala samverkansorgan och resterande 92 är kommunala myndigheter. Tillsynsobjekten som granskats har valts då de utför löpande lagstadgade förvaltningsuppgifter, inbegripet personuppgiftsbehandlingar, inom landskapet Åland. Det bör erinras att listan inte är fullständig, och att det finns såväl kommunala organ och organ under landskapsregeringen som ej vid detta tillfälle varit under granskning. Även organ som ej granskats vid detta tillfälle har en skyldighet att utnämna dataskyddsombud.[1]

En sammanställning av vilka kategorier de aktuella tillsynsobjekten faller in under finns bifogad denna rapport.[2] Totalt har 87 av de 102 tillsynsobjekten utsett dataskyddsombud, merparten av dessa har anlitat dataskyddsombud externt (84 tillsynsobjekt). Samtliga tillsynsobjekt som anlitat dataskyddsombud externt har anlitat Åda Ab. Detta är en väsentlig mängd av Datainspektionens tillsynsobjekt enligt Landskapslag (2019:9) om dataskydd inom landskaps- och kommunalförvaltningen (Dataskyddslagen). Det finns således starka skäl att säkerställa att de tjänster som Åda Ab tillhandahåller är tillräckliga för att de personuppgiftsansvariga ska kunna uppfylla skyldigheterna som åligger dem gällande dataskyddsombudets ställning.[3] Därmed har Datainspektionen även granskat tjänsteavtal mellan de berörda tillsynsobjekten och Åda Ab.

De 15 tillsynsobjekt som ännu ej utnämnt dataskyddsombud kommer att bli föremål för ett föreläggande att utnämna dataskyddsombud. Dessa föreläggande kommer med största sannolikhet att expedieras i december 2019, en uppföljning av ärendet gällande de 15 berörda tillsynsobjekten kommer att ske kort efter att svarstiden gått ut. En rapport över denna uppföljning kommer att publiceras på Datainspektionens anslagstavla.

2.2 De olika dataskyddsombudslösningarna

2.2.1 Åda Ab

Åda Ab är ett offentligägt aktiebolag. De tillhandahåller huvudsakligen IT-drift och biträder landskapsregeringens allmänna förvaltning med upphandling av tjänster. En stor del av Landskapets myndigheter, samt även kommunala myndigheter använder Åda ABs tjänster.

Åda AB tillhandahåller även en servicelösning om tillhandahållande av dataskyddsombud. Samtliga kommunstyrelser utom Kökar kommuns kommunstyrelse har beställt dataskyddsombudstjänster av Åda AB.

När avtal tecknades under 2018 var det tre personer som planerades arbeta som dataskyddsombud vid Åda AB, idag finns två personer som utför tjänsten.

[1] Se Dataskyddsförordningen artikel 37.1 a)
[2] Se bilaga Sammanställning.pdf
[3] Se Dataskyddsförordningen artikel 38

Totalt har dataskyddsombuden 84 huvudmän/personuppgiftsansvariga som omfattades av denna granskning. Det är sannolikt att flera av de tillsynsobjekt som ännu ej formellt utnämnt dataskyddsombud ämnar utse Åda Ab som dataskyddsombud.

Så som avtalen är skrivna är tjänsten timbaserad, där mindre organisationer köper färre timmar och större organisationer ibland hela tjänster.

Landskapsregeringens allmänna förvaltning köper idag 1,5 årsverken.[4] Underliggande myndigheter har genom tillägg till grundavtalet upprättat under sommaren 2019 möjlighet att ta del av dessa tjänster.[5]

Ålands Hälso- och Sjukvård köper idag 1 årsverke av Åda Ab.[6]

Kommunerna har blivit erbjudna att köpa timmar av Åda Ab för 70 €/h. De mindre kommunerna (600 medlemmar eller mindre) köper en timme per kommun. Ingen kommun köper idag mer än 5 timmar i månaden enligt sitt grundavtal. Totalt köper kommunerna 32,5 timmar per månad.[7]

De kommunala samverkansorganen köper enligt avtal 9 timmar per månad.

2.2.2 Intern lösning

När granskningen inleddes fanns det två kommuner som valt att anställa ett dataskyddsombud internt. Det fanns, då granskningen inleddes, enbart beslut ifrån kommunstyrelser eller tjänstemän för dessa utnämnanden.

Under granskningens förlopp övergick dock en av kommunerna till att köpa tjänster av Åda Ab. I skrivande stund finns således enbart en kommun som har anlitat dataskyddombud internt.

Det ska erinras att det inte finns några hinder mot att utnämna dataskyddsombud internt och att ett dataskyddsombud enligt dataskyddsförordningen kan ha andra uppdrag vid sidan av uppdraget som dataskyddsombud. Det åligger dock den personuppgiftsansvarige att säkerställa att det inte uppstår intressekonflikter mellan de olika uppdragen.

Om en intern lösning ska användas är det därför att rekommendera att rollen kombineras med en roll som typiskt sett inte innebär mandat att fatta beslut om verksamheten, till exempel verksamhetsutvecklare eller någon form av supporttjänst (jurist, IT-support eller dylikt).

2.3 Datainspektionens slutsatser av granskningen

Trots att dataskyddsombud blivit utnämnda och deras uppgift är att övervaka efterlevnaden av Dataskyddsförordningen[8] har dessa inte informerat sina huvudmän om hur personuppgiftsansvaret är fördelat i deras organisationer. Datainspektionen har i vart fall inte tagit del av någon information av detta slag ska ha delgivits kommunerna eller landskapsregeringens allmänna förvaltning.

Konsekvensen av att de flesta myndigheter och organ inom Ålands offentliga förvaltning först under 2019 utnämnt dataskyddsombud är att dataskyddsombuden inte tidigare haft något mandat att ta del av uppgifter hos de organ som ej utnämnt dataskyddsombud.

[4] Se bilaga DPO-avtal LR.pdf
[5] Se bilaga tillägg grundavtal DPO-tjänst LR.pdf
[6] Se bilaga DPO-avtal ÅHS.pdf
[7] Se bilaga Timlista Åda DPO-tjänster kommunal.PNG och bilaga DPO-avtal Mariehamn.pdf
[8] Se dataskyddsförordningen artikel 39 1. b)

Det kan konstateras att enbart ett fåtal av granskningsobjekten i denna undersökning på eget bevåg anmält sitt dataskyddsombuds kontaktuppgifter till Datainspektionen, trots den formella skyldigheten att göra detta i dataskyddsförordningens artikel 37. Detta tyder på en avsaknad av förståelse hos tillsynsobjekten gällande deras skyldigheter under gällande dataskyddslagstiftning och en definitiv brist i deras kommunikation med dataskyddsombuden.

Det åligger samtliga personuppgiftsansvariga under Datainspektionens tillsyn att delge Datainspektionen kontaktuppgifter till sitt dataskyddsombud. När granskningen inleddes hade enbart 22 tillsynsobjekt delgivit datainspektionen kontaktuppgifter till sitt/sina dataskyddsombud. Det bör i sammanhanget erinras återigen att den bifogade sammanställningen inte omfattar Datainspektionens samtliga tillsynsobjekt. Även övriga tillsynsobjekt har en skyldighet att delge Datainspektionen kontaktuppgifter till sitt eller sina dataskyddsombud. Tillsynsobjekt som detta berör är bland annat organisationer som biträder myndigheter med offentliga förvaltningsuppgifter, till exempel inom området för socialvård,[9] eller organ som sysslar med verksamhet inom åländsk behörighet som ej är myndigheter[10]. Osäkerhet om vad som faller inom åländsk behörighet kontra rikets behörighet samt osäkerhet kring hur personuppgiftsansvariga organ ska identifieras inom Ålands offentliga förvaltning är de sannolika förklaringarna till detta låga antal delgivningar.

Kommunernas avtal med Åda Ab är timbegränsat, till högst fem timmar per månad för de största kommunerna, även de kommunala samarbetsorganen har ett kraftigt begränsat timantal per månad att förfoga över. Den låga timmängden köpt av kommuner och kommunala samarbetsorgan torde göra det svårt för de berörda personuppgiftsansvariga att hålla sig inom avtalets gränser och samtidigt uppfylla sin skyldighet enligt förordningen att involvera dataskyddsombudet i alla frågor som rör skyddet för personuppgifter.[11] Det fordras vidare utredning för att avgöra säkert i vilken omfattning dataskyddsombuden involveras i frågor som rör deras ansvarsområden

En risk som identifierats i samband med granskningen är att dataskyddsombuden vid Åda Ab riskerar att hamna i jävssituationer detta då de arbetar vid ett företag som i omfattande mängd biträder dataskyddsombudens huvudmän i personuppgiftsbehandlingar. Det är den personuppgiftsansvariges ansvar att säkerställa att dataskyddsombuden inte utför uppdrag vid sidan av sina åtaganden som dataskyddsombud hos den personuppgiftsansvarige som kan leda till intressekonflikt.[12]

3 Rekommendationer

Följande är rekommendationer riktade till de myndigheter som nyttjar Åda Ab som dataskyddsombud då det identifierats eventuella problem eller risker som innebär att de personuppgiftsansvariga myndigheterna svårligen kan uppfylla sina skyldigheter under dataskyddsförordningens artikel 38 på ett tillräckligt sätt.

Dessa risker gäller i huvudsak den köpta tjänstens omfattning, risk för intressekonflikter eller instruktioner till dataskyddsombudet samt antalet tjänster som Åda Ab säljer.

[9] Se Dataskyddslagen 1 kap. 2 § och Landskapslag (1995:101) om tillämpning i landskapet Åland av riksförfattningar om socialvård.
[10] Landskapslag (2019:74) om tillämpning på Åland av riksförfattningar om dataskydd.
[11] Se dataskyddsförordningen Artikel 38 1.
[12] Se dataskyddsförordningen Artikel 38 6.

3.1 Avtalets omfattning

I Datainspektionens slutsatser av granskningen identifieras ett huvudsakligt problem som kan innebära hinder för kommunala personuppgiftsansvariga gällande regelefterlevnaden av dataskyddsförordningen. Nämligen att de inte köper tillräckligt mycket timmar från Åda Ab för att kunna involvera dataskyddsombuden i alla ärenden som rör skyddet av personuppgifter.

Konsekvensen blir att dataskyddsarbetet hos den personuppgiftsansvarige blir begränsat till timantal istället för behov. Behovet av stöd från dataskyddsombuden kan svårligen uppskattas till ett exakt antal timmar per månad, eftersom dataskyddsarbetets omfattning påverkas av omständigheter som inte alltid kan förutses. En begränsning av antalet timmar i avtalet skapar även incitament hos den personuppgiftsansvarige att begränsa kontakten med dataskyddsombudet. Då nödvändigt arbete utöver timbegränsningen riskerar att innebära merkostnader för den personuppgiftsansvarige.

Datainspektionens uppfattning är att Åda Ab:s avtal med sina kommunala huvudmän inte är lämpligt för att säkerställa att dataskyddsombuden faktiskt ges tillräcklig tid för att utföra sina uppgifter.

Datainspektionen rekommenderar därför att de avtal som är timbegränsade i sin omfattning omförhandlas att radera eventuell timbegränsning i avtalet. Tillsynsobjekten rekommenderas istället att upphandla en ej timbegränsad tjänst till fast pris. Det åligger de berörda avtalsparterna att uppskatta en skälig kostnad, samt att omförhandla avtalet vid behov.

3.2 Intressekonflikter och mottagande av instruktioner

Det är Datainspektionens förståelse att Åda Ab biträder myndigheter med olika personuppgiftsbehandlingar. Det är oklart i vilken omfattning de berörda personuppgiftsansvariga har vidtagit åtgärder för att begränsa eventuella intressekonflikter som dataskyddsombuden kan eventuellt kan bli föremål för. Det bör även erinras att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet inte tar emot instruktioner för utförandet av uppgifterna som dataskyddsombud. Då tjänsten köps på sätt som görs i förevarande fall erfordras någon form av garanti av den säljande parten för att säkerställa att intressekonflikter elimineras och att dataskyddsombuden inte tar instruktion från sin arbetsgivare för hur uppgifterna ska skötas gentemot kunden.

Datainspektionen rekommenderar därför att personuppgiftsansvariga som nyttjar Åda Ab för fler tjänster än de som dataskyddsombud begär att Åda Ab redogör för hur de säkerställer att dataskyddsombuden inte riskerar att hamna i intressekonflikter, samt att berörda personuppgiftsansvariga begär att Åda Ab lämnar garantier för att säkerställa att ingen inom Åda Ab ger instruktioner till dataskyddsombuden vid utförandet av deras uppgifter. Alternativt att de personuppgiftsansvariga som biträdes av Åda Ab i personuppgiftsbehandlingar häver avtalet om dataskyddsombud med Åda Ab och löser utnämningen av dataskyddsombud på annat sätt.

3.3 Antalet tjänster hos Åda Ab

Åda Ab är bundna genom avtal att tillhandahålla 2,5 årsarbetstider plus ca 40 timmar per månad. Det finns trots detta enbart två personer hos Åda Ab som arbetar som dataskyddsombud åt de personuppgiftsansvariga som tecknat avtal med Åda Ab.

Givet det omfattande ansvaret att involvera dataskyddsombudet i frågor som rör dataskydd och givet det relativt mångfacetterade område som Ålands offentliga förvaltning arbetar under är det även osannolikt att två personer skulle ha möjlighet bistå och granska samtliga personuppgiftsansvariga och deras behandlingar på så vis som åligger dataskyddsombuden enligt dataskyddsförordningen.

Datainspektionens rekommendation är därför att de personuppgiftsansvariga som tecknat avtal med Åda Ab kräver att Åda Ab säkerställer att de har personal för att täcka samtliga tjänster de säljer. Alternativt att de personuppgiftsansvariga som tecknat avtal med Åda Ab säger upp avtalet med Åda Ab, då Åda Ab inte uppfyller sina åtaganden i dagsläget.

4 Förelägganden

De tillsynsobjekt i granskningen som inte utnämnt dataskyddsombud kommer att bli föremål för förelägganden att utnämna ett sådant. Dessa förelägganden kommer att delges dessa tillsynsobjekt särskilt.

5 Uppföljning

Datainspektionen kommer att genomföra en uppföljning av denna granskning under 2020 för att undersöka om de rekommendationer som givits i avsnitt 3 följs och för att uppdatera sammanställningen av utnämnande av dataskyddsombud efter förelägganden enligt avsnitt 4 delgivits de berörda parterna.

Granskningen utförd av Datainspektionens myndighetschef: Joakim Söderberg.

6 Bilagor

1. Sammanställning.pdf
2. DPO-avtal LR.pdf
3. tillägg grundavtal DPO-tjänst LR.pdf
4. DPO-avtal ÅHS.pdf
5. Timlista Åda DPO-tjänster kommunal.PNG
6. DPO-avtal Mariehamn.pdf