Årsrapport från dataskyddsombudet

Dataskyddsarbetet 2019 för stadsbyggnadsnämnden

Mottagare: Stadsbyggnadsnämnden
Dnr: SBN 2020/127-19
Datum: 2020-03-04
Dokumentansvarig: Anna Brantberger, dataskyddsombud

Innehåll

1 Inledning

1.1 Bakgrund

Den personuppgiftsansvarige är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige är därmed den som har det yttersta ansvaret för all behandling av personuppgifter. Personuppgiftsansvarig i Täby kommun är respektive nämnd och bolag.

Dataskyddsombudet (DSO) är den fysiska person som, efter förordnande av den personuppgiftsansvarige, bland annat har till uppgift att lämna råd och stöd till den personuppgiftsansvarige samt kontrollera att dataskyddslagstiftningen följs inom organisationen. Detta sker exempelvis genom att DSO utför kontroller och informationsinsatser.

Aktuell rapport beskriver huvuddragen av det dataskyddsarbete samtliga nämnder och bolag i kommunen har utfört under det gångna verksamhetsåret.

1.2 Lagkrav

Dataskyddsförordningen trädde i kraft den 25 maj 2018 och innebär en rad förändringar i personuppgiftshanteringen. Bestämmelserna i dataskyddsförordningen syftar till att skydda enskildas grundläggande rättigheter och friheter, dvs. rätten till ett privatliv. Dataskyddsförordningen har ersatt personuppgiftslagen, PuL, och är inom flertalet områden mer omfattande.

I enlighet med artikel 38.3 i dataskyddsförordningen ska DSO rapportera om dataskyddsarbetet till den personuppgiftsansvariges högsta förvaltningsnivå, vilket sker genom denna årsrapport.[1]

2 Regelefterlevnad

2.1 Granskningar

För att det ska vara tillåtet att behandla personuppgifter ska det finns en så kallad laglig grund för personuppgiftsbehandlingen. Det finns enligt dataskyddsförordnigen sex lagliga grunder och en av dem är samtycke.[2] Samtycke innebär att den individ, vars personuppgifter nämnden eller bolaget behandlar, har medgett att personuppgifterna får behandlas för ett eller flera specifika ändamål. Samtycket ska vara frivilligt och kravet på hur ett samtycke ska vara utformat finns specificerat i dataskyddsförordningen.

Eftersom Datainspektionen i sin tillsynsplan för åren 2019-2020[3] annonserade att samtycke är en prioriterad rättsfråga beslutade DSO att granska samtliga nämnders och bolags användning av den lagliga grunden samtycke för behandling av personuppgifter under våren 2019. Den sammanfattande bedömningen av granskningen var att nämnderna och bolagen, inom det granskade området, i allt väsentligt hade en god anpassning till de krav som följer av dataskyddslagstiftningen. Samtliga rekommendationer som DSO gav efter granskningen är åtgärdade.

Under december månad har ytterligare en granskningsinsats påbörjats. Denna avser ett urval av upprättade personuppgiftsbiträdesavtal i kommunen, vilket är avtal som upprättas när en leverantör behandlar personuppgifter för nämndens eller bolagets räkning. Granskningen är planerad att avslutas under våren 2020.

[1] Se Riktlinjer för dataskyddsombud s 18 i WP 243.
[2] Jfr artikel 6 dataskyddsförordningen.
[3] Se Tillsynsplan 2019-2020, dnr DI-2019-841, beslutsdatum 2019-03-19, s 2.

3 Registerutdrag, rättelse och radering

3.1 Bakgrund

Dataskyddsförordningen har medfört att olika typer av rättigheter har tillkommit för de personer som nämnder och bolag behandlar personuppgifter om. Sådan person har exempelvis rätt att kostnadsfritt få en sammanställning över de personuppgifter som nämnden eller bolaget har lagrat beträffande denne (s.k. registerutdrag[4]). Vidare har nämnden eller bolaget en skyldighet att tillse att felaktiga personuppgifter korrigeras eller kompletteras vid behov (s.k. rätt till rättelse[5]). Nämnder och bolag har också en skyldighet att radera personuppgifter (s.k. rätt att bli raderad[6]). Detta är dock ingen absolut rättighet som gäller i alla sammanhang.

3.2 Uppdaterad process

En begäran om registerutdrag, rättelse eller radering kan inkomma till en nämnd eller till ett bolag i kommunen när som helst. Det är därför viktigt att ha en klar process för hur det ska gå till när man till exempel tar fram information om en person och lämnar ut den. I Täby kommun är det möjligt att begära registerutdrag, rättelse eller radering både digitalt och manuellt.

Under året har processen för hur en begäran om registerutdrag, rättelse eller radering ska hanteras uppdaterats för att dessa förfrågningar ska kunna handläggas på ett mer effektivt sätt. Ett registerutdrag ska enligt dataskyddsförordningen lämnas ut inom 30 dagar från begäran därom och rättelse eller radering ska ske utan onödigt dröjsmål.

3.2.1 Statistik registerutdrag, rättelser och radering

Under år 2019 har totalt 36 ärenden inkommit via E-tjänsten för personuppgiftshantering. Av dessa ärenden var fem regelrätta begäran om registerutdrag. En avsåg samtliga nämnder och en avsåg samtliga nämnder förutom Stadsbyggnadsnämnden och Kultur- och fritidsnämnden. Resterande begäran om registerutdrag avsåg Barn- och grundskolenämnden samt Gymnasie- och näringslivsnämnden (3), Kommunstyrelsen (1) och Socialnämnden (1). Samtliga begäran om rättelser avsåg Barn- och grundskolenämnden och inkommen begäran om radering avsåg Gymnasie- och näringslivsnämnden. Resterande inkomna ärenden har exempelvis avsett begäran om allmän handling (3) eller frågor kopplade till andra verksamheter inom kommunen.

Antal begäran om registerutdrag	
2019	5
2018	4

Antal begäran om rättelse	
2019	8
2018	9

Antal begäran om radering	
2019	1
2018	0

[4] Jfr artikel 12 och 15 dataskyddsförordningen.
[5] Jfr artikel 16 dataskyddsförordnigen.
[6] Jfr artikel 17 dataskyddsförordnigen. Denna rättighet är även känd som "rätten att bli glömd".

4 Övriga aktiviteter

4.1 Sammanfattning av övriga aktiviteter 2019

För att samtliga nämnder och bolag ska kunna bedriva ett systematiskt och kvalitativt dataskyddsarbete krävs att relevant information finns lätt tillgänglig för verksamheterna. Under året har därför en ny intern webbsida lanserats gällande information om personuppgiftshanteringen inom kommunen, i syfte att stötta verksamheterna att göra rätt.

Eftersom dataskyddsförordningen ställer höga krav på dokumentation och då den personuppgiftsansvarige ska kunna visa att lagen efterlevs har arbetet med att ta fram styrande och stödjande dokument fortsatt. De dokument som tagits fram under året avser bland annat personuppgiftsbiträdesavtal, webbpubliceringar av nämndhandlingar där personuppgifter ingår, mall för konsekvensbedömning samt mall för utredning av personuppgiftsincidenter.

Under året har en kartläggning av alla gemensamma IT-system genomförts och en rättsakt arbetats fram, vilken reglerar personuppgiftshanteringen och personuppgiftsansvaret mellan samtliga nämnder inom kommunen. Arbetet med att (där behov finns) komplettera och uppdatera befintliga avtalsrelationer med personuppgiftsbiträdesavtal fortgår. Likaså att tillse att personuppgiftsbiträdesavtal upprättas vid behov när nya avtal tecknas med leverantörer. En särskild kontrollpunkt avseende personuppgiftsbiträdesavtal har också implementerats i upphandlingsenhetens upphandlingsprocess.

Slutligen har arbetet med att genomföra konsekvensbedömningar[7] vid personuppgiftsbehandlingar som innebär hög risk[8] påbörjats och en process för detta har arbetats fram. Att vidta en konsekvensbedömning är dels ett sätt för den personuppgiftsansvarige att visa att dataskyddsförordningen följs, dels ett sätt att komma fram till lämpliga åtgärder för att skydda och minska risken för personuppgifterna som behandlas. En särskild kontrollpunkt avseende behov av konsekvensbedömning har också implementerats i Täby kommuns generella projektmodell samt i upphandlingsenhetens upphandlingsprocess.

4.2 Interna utbildningar

Dataskyddsförordningen som helhet är ett komplicerat regelverk som ställer krav på alla inblandade parter, såväl personuppgiftsansvariga som personuppgiftsbiträden. Om regelverket inte följs finns risk för sanktionsavgifter, skadeståndskrav samt andra sanktioner vilket kan innebära risker för verksamheterna. Det är därför av stor vikt att Täby kommun fortsätter upprätthålla en hög medvetenhet hos alla anställda avseende aktuell lagstiftning och styrande dokument om dataskydd.[9] Att kontinuerligt vidta kompetenshöjande åtgärder är därför en nödvändig del av det fortsatta arbetet med dataskyddsfrågorna inom kommunen.

Mot denna bakgrund har det under år 2019 genomförts utbildningsinsatser riktade såväl mot samtliga verksamhetsområden som vissa specifika funktioner inom kommunen och även externa samarbetsparter.[10] Den generella utbildningsinsatsen för samtliga anställda beträffande dataskydd i offentlig verksamhet genomfördes under perioden september-oktober. Totalt genomförde 54 procent av alla anställda utbildningen.[11] Denna siffra kan jämföras med 81 procent år 2018.

---

[7] Jfr artikel 35.1 dataskyddsförordningen.

[8] Jfr artikel 35.1, illustrerat av artikel 35.3 och kompletterat av artikel 35.4 dataskyddsförordningen.

[9] I Datainspektionens rapport 2019:3, Anmälda personuppgiftsincidenter januari–september 2019 s 12, understryks behovet av utbildning eftersom den vanligaste orsaken till inrapporterade personuppgiftsincidenter är den mänskliga faktorn, vilket i många fall kan bero på att medarbetarna inte känner till fastställda rutiner tillräckligt bra.

[10] De specifika funktioner internt som utbildats är dataskyddsorganisationen, upphandlingsenheten och enheten för stöd och service. Efter önskemål har utbildning också hållits för specifika funktioner inom Barn- och grundskolenämnden såsom rektorer, ledningsgrupp, lärare och fritidspersonal samt för privata utförare inom Kultur- och fritidsnämnden.

[11] Utbildningen kunde genomföras dels via utbildningsverktyget, dels genom muntlig utbildning av dataskyddsorganisationen.

4.2.1 Statistik dataskyddsutbildning

Verksamhetsområde	Deltagande i procent	
	2018	**2019**
Kommunledningskontoret	77	67
Samhällsutvecklingskontoret	88	59
Social omsorg	77	46
Kultur och fritid	90	37
Utbildning	82	55
SRMH	100	68

5 Personuppgiftsincidenter

5.1 Rapporteringsskyldighet till Datainspektionen

Av dataskyddsförordningen följer en skyldighet för nämnder och bolag att rapportera vissa personuppgiftsincidenter till Datainspektionen.[12] En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Alla incidenter är inte rapporteringspliktiga till Datainspektionen. Dock måste samtliga incidenter dokumenteras av den personuppgiftsansvariga nämnden eller bolaget.

5.2 Utvecklad incidenthanteringsprocess

Processen för personuppgiftsincidenthantering har utvecklats ytterligare för att säkerställa att personuppgiftsincidenter bedöms på ett likartat sätt oavsett var, när och hur incidenten inträffar. En mall för utredning av inträffade incidenter har arbetats fram för att uppnå en likartad bedömning. Samma mall utgör även underlag med anledning av dokumentationsplikten som ankommer på den personuppgiftsansvarige.

5.3 Statistik personuppgiftsincidenter

Under året har totalt 25 personuppgiftsincidenter anmälts varav tre har rapporterats vidare till Datainspektionen, vilket kan jämföras med fem anmälningar totalt under år 2018 varav samtliga rapporterades vidare till Datainspektionen. Att antalet dokumenterade incidenter har ökat beror troligtvis på en ökad medvetenhet och kunskap om anmälningsskyldigheten och att rutinerna för att anmäla incidenter blivit mer etablerade.

Att en nämnd eller ett bolag anmäler många personuppgiftsincidenter behöver dock inte vara en indikation på bristande säkerhet. Tvärtom kan det tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

Personuppgiftsansvarig	Dokumenterade incidenter		Anmälda incidenter		Återkoppling från Datainspektionen	
	2018	**2019**	**2018**	**2019**	**2018**	**2019**
Stadsbyggnadsnämnden	-	1	-	-	-	-

[12] Jfr artikel 33 dataskyddsförordningen.