Årsrapport från dataskyddsombudet

Dataskyddsarbetet 2022 för Södra Roslagens miljö- och hälsoskyddsnämnd

Trygghets- och säkerhetsenheten
Desirée Widman
2023-02-10
Dnr SRMH 2023-197.1210

Innehåll

1. Inledning

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.

I Täby kommun är respektive nämnd och bolag eget personuppgiftsansvarig.

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 med fokus på de kommunövergripande processerna.

Lagkrav

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. Riktad granskning

2.1. Personuppgiftsbiträdesavtal

Under året 2022 har två dokumenterade kontroller utifrån kommunledningskontorets interna kontrollplan inom området dataskydd genomförts för samtliga nämnder. Nämndernas förmåga att upprätta personuppgiftsbiträdesavtal (PUB-avtal), när personuppgiftshantering förekommer i avtalsrelationen, har kontrollerats. Totalt har 53 leverantörsavtal kontrollerats.

[1] Se Riktlinjer för dataskyddsombud s 18 i WP 243.

Utfallet av kontrollerna har visat att det saknats personuppgiftsbiträdesavtal i 4 av 53 kontrollerade leverantörsavtal. Berörda verksamhetsrepresentanter är informerade om bristen och rekommenderade att åtgärda avsaknaden av personuppgiftsbiträdesavtal.

2.1.1. Informationsinsatser kopplat till upprättande av personuppgiftsbiträdesavtal

En extra kommunikationsinsats kring vikten av att teckna personuppgiftsbiträdesavtal genomfördes under januari 2022 med chefer inom tjänstemannaorganisationen som målgrupp. Både som riktad information i mail och som information på Täby kommuns intranät Insidan.

Riktad utbildning i hantering av PUB-avtal för upphandlare på inköpsenheten och samordnaren för avropsinköp från licenspartneravtal har genomförts.

I samband med det informationsklassningsarbete som pågår för att lyfta kommunens informationssäkerhet generellt så diskuteras vikten av korrekt upprättade personuppgiftsbiträdesavtal med nyckelpersoner inom de olika verksamhetsområdena.

2.2. Riskbedömning

Dataskyddsombudet bedömer att insatta utbildningsinsatser har gett effekt och att det finns en ökad medvetenhet om upprättandet av korrekta avtalshandlingar. Risken att personuppgiftsbiträdesavtal i stor utsträckning saknas i avtal är låg för digitala verksamhets- och stödsystem upphandlade enligt lagen om offentlig upphandling (LOU).

Fortsatt kvarstående risk kan dock noteras vid förnyelser av leverantörsavtal där aktuell verksamhet inte tar tillfället i akt att se över och revidera avtalsinnehållet.

Dataskyddsombudet rekommenderar att uppföljning av förmågan att upprätta personuppgiftsbiträdesavtal i fortsättningen ingår i internkontrollen gällande informationssäkerhetkrav. Upprättande av personuppgiftsbiträdesavtal är en del i informationssäkerhetskravställningen vid upphandling/avtalstecknande.

3. Registerutdrag, rättelse och radering

3.1. Bakgrund

De personer som nämnder och bolag behandlar personuppgifter om har till exempel rätt att kostnadsfritt få en sammanställning över de personuppgifter som nämnden eller bolaget har lagrat beträffande denne (s.k. registerutdrag[2]). Vidare har nämnden eller bolaget en skyldighet att tillse att felaktiga personuppgifter korrigeras eller kompletteras vid behov (s.k. rätt till rättelse[3]). Nämnder och bolag har också en skyldighet att radera personuppgifter (s.k. rätt att bli raderad[4]). Detta är dock ingen absolut rättighet som gäller i alla sammanhang.

3.1.1. Statistik registerutdrag, rättelser och radering

Under året har totalt 32 ärenden inkommit via e-tjänsten för personuppgiftshantering.

Av dessa ärenden var endast en regelrätt begäran om registerutdrag. Den inkomna begäran om registerutdrag avsåg både kommunstyrelsen och kultur- och fritidsnämnden. Vidare inkom en regelrätt begäran om rättelse. Den avsåg barn- och grundskolenämnden.

Resterande inkomna ärenden har exempelvis avsett begäran om allmän handling eller verksamhetsfrågor så som ansökan om förskole- och skolplacering eller hjälp med studie- och yrkesvägledning inom ramen för vuxenutbildning .

Tabell nr 1. Registerutdrag, rättning och radering

År	Antal begäran om registerutdrag	Antal begäran om rättelse	Antal begäran om radering
2022	**1**	**1**	**0**
2021	*2*	*2*	*0*
2020	*2*	*6*	*0*
2019	*5*	*8*	*1*
2018	*4*	*9*	*0*

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

3.1.2. Riskbedömning

Dataskyddsombudet anser att de kommunövergripande rutinerna för hantering av registerutdrag, rättelse och radering uppfyller lagstiftningens krav och hanteras därefter. Ingen risk föreligger som hindrar de registrerade att utöva sina rättigheter.

4. Personuppgiftsincidenter

Dokumentation av personuppgiftsincidenter är av stor betydelse i syfte att kunna visa på efterlevnad av dataskyddsförordningen. Personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter och även leda till förtroendeskada för den personuppgiftsansvarige.

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.

Det är viktigt att alla medarbetare är insatta i hur man ska agera om man misstänker en personuppgiftsincident. Stöd för personuppgiftsincidentanmälan finns på intranätet under Hantering av personuppgifter.

4.1. Rapporteringsskyldighet till Integritetsskyddsmyndigheten

Av dataskyddsförordningen följer en skyldighet för nämnder och bolag att rapportera vissa personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY).[5]

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

4.2. Statistik personuppgiftsincidenter

Under 2022 har totalt 28 personuppgiftsincidenter dokumenterats för kommunens samtliga nämnder och bolag. 10 har rapporterats vidare till IMY. IMY har återkopplat gällande samtliga rapporterade incidenter med bedömningen att anmälda ärenden inte är av den grad att de behöver öppna ett tillsynsärende. Ärendena har därefter avslutats.

IMY använder sedan i sin tur de inrapporterade incidenterna för framtagande av

[5] Jfr artikel 33 dataskyddsförordningen.

statistikrapporter med syftet att sprida kunskap om var riskerna att incidenter inträffar är störst.

Orsaken till de flesta incidenter som rapporteras beror på den mänskliga faktorn och felhantering i det enskilda fallet. Kommunikation via mail/utskicksfunktioner som skickats till fel mottagare är den allra vanligaste incidenten. I IMYs statistikrapport från 2020 framkommer att den mänskliga faktorn står för 51% av alla incidenter.

För Södra Roslagens miljö- och hälsoskyddsnämnd har två internt dokumenterade personuppgiftsincidenter med ringa påverkan rapporterats under året, båda kopplade till hanteringsrutiner vid utskick.

Tabell nr 2. Dokumenterade och rapporterade personuppgiftsincidenter

År	Internt dokumenterade personuppgiftsincidenter	Rapporterade personuppgiftsincidenter till IMY
2022	**2**	**-**
2021	-	-
2020	*1*	-
2019	-	-
2018	-	*1*

4.3. Riskbedömning

Personuppgiftsincidenter kan innebära betydande eller allvarliga konsekvenser för enskilda personer, kommunen som helhet, andra myndigheter och organisationer.

Medarbetarnas hantering av information är av största vikt för att inte incidenter ska uppstå. Den mänskliga faktorn är oftast det största hotet.

Dataskyddsombudet rekommenderar att personuppgiftsansvariga tillser att arbete fortgår med att utbilda all personal i informationshantering för att medvetandegöra hur personuppgifter får hanteras. Det är den enskilt viktigaste insatsen för att reducera antalet personuppgiftsincidenter.

5. Övriga aktiviteter

5.1. Informationssäkerhet och dataskydd

För att uppfylla dataskyddsförordningens krav på dataskydd behövs en helhetssyn avseende det systematiska arbetet med informationssäkerhet, it-säkerhet, cybersäkerhet och personuppgiftshantering. En viktig del i det arbetet är också att bedriva kommunikations- och utbildningsinsatser för att förankra innehåll i övergripande styrdokument, höja kunskapen om säkert beteende samt öka förståelsen för de konsekvenser som kan uppstå om incidenter inträffar. Effekten av incidenter kan bland annat bli att information som omfattas av sekretess eller innehåller andra känsliga personuppgifter tillgängliggörs för obehöriga, att viktig informations korrekthet påverkas eller att information inte är tillgänglig för verksamheten i förväntad utsträckning och inom önskad tid.

Inom Trygghets- och säkerhetsenheten finns dataskyddssamordnarfunktioner, dataskyddsombudet och informationssäkerhetssamordnare organiserade. Dataskyddssamordnarna är de stödjande operativa resurser som hjälper de personuppgiftsansvariga nämnderna och bolagen i Täby kommun att driva på det systematiska arbetet med dataskyddsfrågor. Dataskyddsombudet har en rådgivande och granskande roll.

Med början under 2021 och fortsättning under hela 2022 har dataskyddsamordnare och informationssäkerhetssamordnare arbetat nära varandra för att väva ihop kommunens övergripande systematiska arbete med informationssäkerhet och dataskydd.

5.1.1. Styrdokument

Under 2022 har en översyn av styrdokumenten gjorts, flertalet har renskrivits i Täby kommuns nya tillgänghetsanpassade dokumentmall.

En *Anvisning för hantering av e-post* har omarbetats och fastställts, ett viktigt stöddokument som ska vägleda medarbetare och förtroendevalda i Täby kommun att hantera personuppgifter på rätt sätt vid hantering av e-post. Denna har också kommunicerats via intranätet Insidan till alla medarbetare och chefer.

Dataskyddsombud, dataskyddssamordnare och informationssäkerhetsamordnare har under 2022 arbetat fram ett förslag till riktlinjer för informationssäkerhet där effekten av efterlevnaden också kommer ha stor inverkan på det systematiska dataskyddsarbetet.

5.1.1.1. Kamerabevakning

Dataskyddsförordningen är det huvudsakliga regelverket vid kamerabevakning. Kamerabevakningslagen gäller dessutom vid övervakning av ytor dit allmänheten har tillträde och den typen av övervakning är tillståndspliktigt. IMY är tillsynsmyndighet. Under året har stödmaterialet om kamerabevakning som är riktat till verksamheterna setts över och uppdaterats.

5.1.2. Interna utbildningar

Kompetenshöjande åtgärder för medarbetare är en nödvändig del av arbetet med dataskydd inom kommunen och sker också löpande. Utbildningsinsatser har genomförts, både avsedda för hela verksamhetsområden som vissa specifika funktioner inom kommunen. Ett flertal cybersäkerhetsincidenter som under året uppstått hos andra kommuner eller privata företag och som kommunicerats i olika mediekanaler understryker vikten av att hålla medarbetare uppdaterade gällande hur man på ett säkert sätt ska förhålla sig till att arbeta med de personuppgiftsansvariges it-system och hantering av information.

5.1.3. Registerförteckning

2021 (efter KPMGs revision) påbörjades en översyn av samtliga nämnders och bolags register över personuppgiftsbehandlingar (registerförteckning) samt befintliga styrdokument för att uppdatera dem generellt och/eller revidera vid behov.

Som en första del genomfördes en ombearbetning av registerförteckningsmallen i befintligt digitalt stödverktyg för att förenkla registreringar av nya personuppgiftsbehandlingar och föra över befintligt register till den nya mallen.

Under ovan arbetsgång framkom det tydligt att det digitala stödverktyg som används för upprättande av registerförteckning inte längre är ändamålsenlig i förhållande till underhåll av registerförteckningarna över tid.

En utvärdering har genomförts av stödverktyg på marknaden och under hösten 2022 fattades beslut om inköp av nytt stödverktyg. I väntan på den nya leverantörens uppdateringar av funktionalitet har registerförteckningarna hanterats i Excel- format. Inläsning av befintlig registerförteckning till det nya stödverktyget planeras till våren 2023.

5.1.4. Schrems II

Mycket tid och resurser har fortsatt lagts ner på att omvärldsbevaka och hantera konsekvenserna av EU-domstolens dom som meddelades under sommaren 2020 (den s.k. Schrems II-domen) och som påverkar Täby kommuns möjligheter att använda sig

av bland annat amerikanska molntjänster. Dataskyddsombudet har stöttat verksamhetsrepresentanter och dataskyddssamordnare i diskussionen om lämpligheten att upprätta avtal med molntjänstleverantörer där personuppgifter kan komma att lagras i tjänster som lyder under amerikans jurisdiktion.

5.2. Riskbedömning

På grund av omsättning av personal inom Trygghets- och säkerhetsenheten har resurserna som arbetar stödjande till kommunens personuppgiftsansvariga tillfälligt minskat, något som på sikt kan leda till att delar av dataskyddsarbetet blir eftersatt.

I och med det förändrade omvärldsläget bör frågan om datasuveränitet och integritetsskydd i förhållande till användandet av molntjänster (det Schrems II-domen belyser) införlivas i kommande it-strategiska beslut.