Årsrapport från dataskyddsombudet

Dataskyddsarbetet 2023 för kultur- och fritidsnämnden

Juridikenheten
Ulrika Eek Eberharter
2024-03-06
Dnr KFN 2024/16-09

Innehållsförteckning

1. Inledning

1.1 Bakgrund

I Täby kommuns verksamheter behandlas dagligen en stor mängd personuppgifter. Att hantera den omfattningen av personuppgifter som anförtrotts kommunen innebär ett stort förtroende att förvalta. *Personuppgifter* är ett brett begrepp som omfattar all information som direkt eller indirekt kan härledas till en fysisk person i livet, såsom namn, personnummer, ljudupptagningar och fotografier. *Behandling* innebär t.ex. insamling, lagring och radering. EU:s dataskyddsförordning[1] (GDPR) blev svensk lag i maj 2018 och fick därmed stor betydelse för behandling av personuppgifter.

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 har respektive nämnd och bolag ett eget personuppgiftsansvar.

Dataskyddsombudet är den fysiska person som, efter förordnande av den personuppgiftsansvarige, bl.a. har till uppgift att lämna råd och stöd till den personuppgiftsansvarige samt kontrollera att dataskyddslagstiftningen följs inom organisationen. Detta sker exempelvis genom utförande av kontroller och informationsinsatser.

Aktuell rapport beskriver huvuddragen av det dataskyddsarbete samtliga nämnder och bolag i kommunen har utfört under det gångna verksamhetsåret 2023 med fokus på de kommunövergripande processerna.

1.2 Lagkrav

Av dataskyddsförordningen framgår att dataskyddsombudet ska rapportera om dataskyddsarbetet direkt till den personuppgiftsansvariges högsta förvaltningsnivå, vilket huvudsakligen sker genom denna årsrapport.[2]

[1] 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.
[2] Art. 38.3 dataskyddsförordningen. Se även Europeiska dataskyddsstyrelsens (EDPBs) Riktlinjer om dataskyddsombud, WP 243, antagna den 13 december 2016 (rev. 5 april 2017), s. 18.

2. Riktad granskning utifrån internkontrollplan

2.1 Bakgrund

Under året har två dokumenterade kontroller genomförts för samtliga nämnder utifrån kommunledningskontorets internkontrollplan för 2023 inom området dataskydd och informationssäkerhet. Rapporterna från granskningarna återfinns under dnr KS 2023/152-04. Granskningen omfattade två kontrollområden avseende dataskydd, dels förekomsten av personuppgiftsbiträdesavtal när sådana behövs, dels risken för personuppgiftsrelaterade incidenter.

Det första området avsåg nämndernas förmåga att upprätta personuppgiftsbiträdesavtal. Det är avtal som behöver ingås mellan kommunen och externa parter (främst leverantörer) när dessa behandlar personuppgifter för nämndernas/bolagens räkning. Totalt har 24 stycken av 2023 års nyanskaffade/förnyade avtal registrerade i Täby kommuns avtalskatalog (sammanlagt 534 stycken per 1 december 2023) bedömts vara relevanta för en granskning av dataskyddskrav (och informationssäkerhetskrav). Av 24 granskade avtal saknades personuppgiftsbiträdesavtal i 5 fall.

Det andra området avsåg risken för personuppgiftsrelaterade incidenter och rutinen för rapportering av sådana har därför granskats.

2.2 Riskbedömning

När det gäller det första området (personuppgiftsbiträdesavtal) noteras, i nyss nämnda rapporter från internkontrollen, att kommunens förbättringsarbete gällande leverantörsrelationer delvis ligger i att få alla verksamheter att arbeta med dataskyddskrav (och informationssäkerhetskrav) vid inköp/upphandling, men främst i att arbeta systematiskt med avtalsuppföljning.

Tecknandet av personuppgiftsbiträdesavtal vid inköp/upphandling bedöms fortfarande vara en trög process som oftast släpar efter trots att centralt stöd i att ta fram avtalet finns och att huvudavtalet inte kan anses giltigt innan personuppgiftsbiträdesavtal är upprättat.

Slutsatsen av granskning av det andra området (personuppgiftsincidenter) är att rutinen för sådana fungerar på ett tillfredställande vis och är dokumenterad i styrande dokument och på Insidan, kommunens intranät. Fel orsakade av den mänskliga

faktorn, såsom felskickade mail, dominerar. Fortsatt kontinuerlig utbildning bedöms därför behöva genomföras för att öka medvetenheten hos alla.

Den kommande revideringen av EU:s NIS-direktiv (”NIS 2 direktivet”) kommer sannolikt att ställa större krav på systematisk incidentrapportering (gällande både personuppgifts- och cybersäkerhetsincidenter) med en tydligare kravbild vad gäller styrning och ägarskap. En arbetsgrupp har tillsatts internt som arbetar fram ett förslag på en förhållandevis lätthanterlig övergripande incidentprocess i enlighet med kommande lagstiftning.

Kontrollområdena finns kvar som interna granskningspunkter även i internkontrollplanen för 2024.

3. Den registrerades rättigheter

3.1 Bakgrund

Dataskyddsförordningen ger de registrerade ett antal rättigheter. Den registrerade har t.ex. rätt att kostnadsfritt få en sammanställning över de personuppgifter som nämnden eller bolaget har lagrat beträffande denne (s.k. registerutdrag).[3] Vidare har nämnden eller bolaget en skyldighet att tillse att felaktiga personuppgifter korrigeras eller kompletteras vid behov (s.k. rätt till rättelse).[4] Nämnder och bolag har också en skyldighet att radera personuppgifter (s.k. rätt att bli raderad/glömd).[5] Detta är dock ingen absolut rättighet som gäller i alla sammanhang.

3.2 Statistik registerutdrag, rättelser och radering

Under året har totalt 30 stycken ärenden inkommit via e-tjänsten för personuppgiftshantering.

Av dessa ärenden var åtta regelrätta begäran om registerutdrag. Vidare inkom en regelrätt begäran om rättelse. Resterande inkomna ärenden har exempelvis avsett begäran om allmän handling eller verksamhetsfrågor såsom ansökan om förskole- och skolplacering.

[3] Artikel 12 och 15 dataskyddsförordningen.
[4] Artikel 16 dataskyddsförordningen.
[5] Artikel 17 dataskyddsförordningen.

Tabell nr 1. Registerutdrag, rättning och radering 2018-2023

År	Antal begäran om registerutdrag	Antal begäran om rättelse	Antal begäran om radering
2023	***8***	***1***	**-**
2022	*1*	*1*	*-*
2021	*2*	*2*	*-*
2020	*2*	*6*	*-*
2019	*5*	*8*	*1*
2018	*4*	*9*	*-*

3.3 Riskbedömning

Dataskyddsombudet anser att de kommunövergripande rutinerna för hantering av registerutdrag, rättelse och radering i huvudsak uppfyller lagstiftningens krav och hanteras därefter.

Att begäran från registrerade hanteras i enlighet med dataskyddsförordningens krav är tätt förbundet med allmänhetens förtroende för hur kommunen hanterar personuppgifter. Brister i hanteringen kan även leda till tillsynsärenden från Integritetsskyddsmyndigheten (IMY), med sanktioner som följd. Det ska noteras att IMY under 2023 har inlett över 200 tillsynsärenden, vilket är en väsentlig ökning från året före, och beslutat om sanktionsavgifter om över 120 miljoner kronor, jämfört med 10 miljoner kronor under 2022. Numera finns även en rätt att överklaga IMY:s beslut, vilket innebär att den registrerades rättigheter har stärkts.[6] Täby kommun har inte varit föremål för IMYs tillsyn.

Dataskyddsombudet vill lyfta att det är viktigt att kontinuerligt säkerställa att de eftersökningar som görs resulterar i en heltäckande bild av de personuppgifter som behandlas. Det bör i synnerhet tas höjd för mer komplicerade (omfattande) förfrågningar om registerutdrag. Under 2024 riktas en utbildningsinsats till de kontaktpersoner för berörda verksamheter som på uppdrag av dataskyddssamordnare kan komma att hantera begäran om registerutdrag.

[6] HFD mål nr 6193-22, HFD mål nr 3691-22.

4. Incidenthantering

4.1 Bakgrund

Av dataskyddsförordningen följer en skyldighet för personuppgiftsansvariga nämnder och bolag att rapportera vissa personuppgiftsincidenter till IMY inom 72 timmar.[7] Alla incidenter är inte rapporteringspliktiga till IMY. Dock måste samtliga incidenter dokumenteras av den personuppgiftsansvariga nämnden eller bolaget.[8]

En incident kan vara vardagliga händelser, som en borttappad telefon, till mer dramatiska händelser, som stora hackerattacker mot den centrala IT-miljön. En personuppgiftsincident definieras enligt dataskyddförordningen som: ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”[9] 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.

Stöd för anmälan av personuppgiftsincident finns på Insidan.

I samband med nytillträdd DSO i september 2023 har vikten av att kontakta dataskyddorganisationen vid misstanke om att incident inträffat belysts på Insidan.

4.2 Statistik personuppgiftsincidenter

Under 2023 har totalt 34 personuppgiftsincidenter dokumenterats för kommunens samtliga nämnder. En av dessa har rapporterats vidare till IMY (p.g.a. dess allvarlighetsgrad). IMY har återkopplat att anmält ärende inte föranleder att de behöver öppna ett tillsynsärende. Ärendet har därefter avslutats.

[7] Artikel 33 dataskyddsförordningen.
[8] Dataskyddsförordningen artikel 33.5.
[9] Artikel 4.12 dataskyddsförordningen.

Tabell nr 2. Dokumenterade och rapporterade personuppgiftsincidenter 2018-2023

År	Internt dokumenterade personuppgiftsincidenter	Rapporterade personuppgiftsincidenter till IMY
2023	***34***	***1***
2022	*18*	*10*
2021	*15*	*4*
2020	*14*	*5*
2019	*22*	*3*
2018	-	*5*

Uppdelning av incidenter per nämnd finns i bilaga 1 till denna rapport. För kultur- och fritidsnämnden har två incidenter dokumenterats under året.

4.3 Riskbedömning

Personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter och även förtroendeskada för den personuppgiftsansvarige och kommunen som helhet.

Dataskyddombudet vill framhålla att en grundförutsättning för hanteringen av personuppgifter är att verksamheterna förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver. Det är viktigt att samtliga medarbetare kan identifiera en personuppgiftsincident och även vet hur de ska agera redan vid *misstanke* om en sådan. Incidenthanteringen, som är både tidskritisk och ofta svårbedömd, sker i samarbete mellan berörd verksamhet och dataskyddsorganisationen. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige säkerställer att rutiner finns för att upptäcka personuppgiftsincidenter. Dataskyddsombudet vill understryka att ett högt antal rapporterade incidenter kan förklaras med en god förmåga att identifiera incidenter.

Dataskyddombudet vill vidare belysa att det är viktigt att skilja rapportering av incidenter till IMY med *dokumentationskravet*. Enligt dataskyddsförordningen ska alla personuppgiftsincidenter dokumenteras, d.v.s. oaktat allvarlighetsgrad och oavsett om incidenten ska rapporteras till IMY eller inte.

5. Övrigt dataskyddsarbete

5.1 Dataskyddsorganisationen och omvärldsbevakning

5.1.1 Bakgrund

Den tekniska utvecklingen skapar nya utmaningar vad gäller skyddet av personuppgifter. Cyberattacker har ökat och artificiell intelligens medför risker, bland annat för den personliga integriteten. Dataskyddsorganisationen följer utvecklingen kring den nya AI-förordningen som gäller i hela EU och som syftar till att reglera AI system. Ett förhållningsätt för AI har tagits fram och tillgängliggjorts på Insidan. Användning av AI i verksamheterna har diskuterats.

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 även 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.

Under året har dataskyddsombud, dataskyddsamordnare och informationssäkerhetssamordnare arbetat nära varandra för att väva ihop kommunens övergripande systematiska arbete med informationssäkerhet och dataskydd. Dataskyddssamordnarna/informationssäkerhetssamordnarna är de stödjande operativa resurser som hjälper de personuppgiftsansvariga att driva på det systematiska arbetet med dessa frågor. På varje enhet där personuppgifter behandlas finns även personer utsedda med syftet att bistå på enhetsnivå. Syftet är att genom dessa personer sprida kunskap ut i organisationen samt att verksamhetsnära frågor ska fångas upp mer effektivt. Det finns planer på att intensifiera detta arbete under 2024.

5.1.2 Riskbedömning

På grund av omsättning av personal inom dataskyddsorganisationen har resurserna som arbetar stödjande till kommunens personuppgiftsansvariga tillfälligt minskat, något som på sikt kan leda till att delar av dataskyddsarbetet blir eftersatt. Det är en rekommendation att personuppgiftsansvariga nämnd eller bolag säkerställer att erforderliga resurser finns.

När det gäller AI är det fortfarande för tidigt för att närmare kunna beskriva en mer exakt omfattning av hur AI kommer att påverka kommunens hantering av personuppgifter. Det kan dock redan nu konstateras att antalet fallgropar är många och att det föreligger en tydligt ökad risk rent generellt för personuppgiftsincidenter vid användningen av AI.

5.2 Interna utbildningar

5.2.1 Bakgrund

Utbildning är den enskilt viktigaste insatsen för att reducera antalet personuppgiftsincidenter. Kompetenshöjande åtgärder för medarbetare är därför en nödvändig del av arbetet med dataskydd inom kommunen och något som sker löpande. På Insidan presenteras utbildningar i dataskydd.

Utbildningsinsatser har genomförts, såväl 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 personuppgiftsansvarigas it-system och hantering av information.

Riktade utbildningar har efterfrågats av flera verksamheter, vilket dataskyddombudet upplever positivt, och kommer fortsatt att genomföras under år 2024.

5.2.2 Riskbedömning

Dataskyddsombudet rekommenderar att personuppgiftsansvariga tillser att arbetet med att utbilda all personal fortgår. Dataskyddsombudsorganisationen kommer fortsatt att tillhandahålla webbaserad utbildning såväl som riktade utbildningar på förfrågan eller vid identifierat behov.

Varje enhet inom kommunen som hanterar personuppgifter i någon form bör med jämna mellanrum göra en översyn över enhetens rutiner och dokumentation kopplade till dataskyddsförordningen. Checklista för detta arbete finns på Insidan.

5.3 Register över personuppgiftsbehandlingar

5.3.1 Bakgrund

Enligt dataskyddsförordningen är det en skyldighet för personuppgiftsansvarig att föra ett register över behandlingar som utförts under dess ansvar. Registerförteckningen är

en central del i hanteringen av personuppgifter eftersom den ger en överblick och kontroll rörande vilka behandlingar som görs inom kommunen. Under 2023 fortsatte arbetet med översyn av registret över behandlingar och inläsning av befintlig registerförteckning till det nya stödverktyget har färdigställts. Arbetet med att kontrollera befintliga behandlingarna i registret fortsätter under 2024.

En närliggande informationskälla är information över kommunens alla behandlingar som finns tillgänglig både på taby.se (de s.k. behandlingskorten). Dessa skall under år 2024 ses över för att uppdateras generellt och revideras vid behov.

5.3.2 Riskbedömning

Dataskyddombudet framhåller vikten av att personerna på enheterna som är involverade i uppdateringen av behandlingsregistret får tid till sitt förfogande för denna uppgift.

5.4 Konsekvensbedömningar

5.4.1 Bakgrund

En konsekvensbedömning måste genomföras för vissa högriskaktiviteter som involverar personuppgifter enligt dataskyddförordningen. Konsekvensbedömningar är ett viktigt kontrollverktyg som hjälper den personuppgiftsansvarige att uppfylla kraven i dataskyddförordningen.

5.4.2 Riskbedömning

Kraven på konsekvensbedömningar är höga och kräver ofta mycket kunskap och engagemang från verksamheten. Dataskyddsombudet anser att det är viktigt att kunskap finns om när en konsekvensbedömning behöver genomföras så att dataskyddsorganisationen kan involveras i tid.

Frånvaro av eller bristfälliga konsekvensbedömningar kan leda till höga sanktionsavgifter och skadestånd. Ett exempel på IMYs tillsyn på området är deras beslut från november 2023 om att utfärda en sanktionsavgift på 300 000 kr mot barn- och utbildningsnämnden i en kommun. Där ansågs det att nämnden inte gjort en nödvändig konsekvensbedömning innan en viss digital skolplattform infördes på ett antal av kommunens skolor.[10]

[10] Beslut efter tillsyn enligt dataskyddsförordningen - Barn- och utbildningsnämnden i Östersunds kommun, dnr IMY-2023-1647, 28 november 2023.

5.5 Dataöverföring till tredjeland

5.5.1 Bakgrund

När det gäller dataöverföringar till tredjeland, dvs länder utanför EU, har läget förändrats så att det nu finns större möjligheter till sådana.

Sommaren 2020 meddelade EU-domstolen en dom (den s.k. Schrems II-domen) som fick betydelse för Täby kommuns möjligheter att använda sig av överföringar av personuppgifter till länder utanför EU, såsom användandet av amerikanska molntjänster. Domen grundade sig i att det amerikanska rättssystemet inte ansågs ge ett tillräckligt skydd för personuppgifter som överförs till USA. Sommaren 2023 fattades ett beslut om det som kallas ”adekvat skyddsnivå”. EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå och det är då möjligt att föra över personuppgifter dit utan något särskilt tillstånd. Dessutom har EU-kommissionen bedömt att skyddsnivån är adekvat i USA, om mottagaren omfattas av det s.k. ”EU-US Data Privacy Framework”.

5.5.2 Riskbedömning

Det återstår att se om möjligheten till tredjelandsöverföringar är av tillfällig eller bestående karaktär. Det behöver fortfarande bedömas om sådana överföringar är lämpliga.

Dataskyddsombudet kommer fortsatt stötta verksamhetsrepresentanter och dataskyddssamordnare i diskussionen om lämpligheten att upprätta avtal med molntjänstleverantörer där personuppgifter kan komma att lagras i tjänster som lyder under amerikansk jurisdiktion.

Bilaga 1. Incidentstatistik

Personuppgiftsincidenter per personuppgiftsansvarig nämnd 2018-2023

Personuppgiftsansvarig nämnd	Internt dokumenterade personuppgiftsincidenter	Rapporterade personuppgiftsincidenter till IMY
Kommunstyrelsen		
2023	**2**	-
2022	-	-
2021	*3*	-
2020	-	-
2019	*8*	*1*
2018	-	-
Kultur- och fritidsnämnden		
2023	**2**	**-**
2022	-	*2*
2021	*1*	-
2020	-	*1*
2019	-	-
2018	-	*1*
Socialnämnden		
2023	**22**	**-**
2022	*11*	*3*
2021	*8*	*3*
2020	*12*	*4*
2019	*7*	-
2018	-	*1*
Barn- och grundskolenämnden		
2023	**3**	**-**
2022	*2*	*4*
2021	*2*	*1*
2020	-	*1*
2019	*7*	*1*
2018	-	*2*
Gymnasie- och näringslivsnämnden		
2023	**1**	**1**
2022	*3*	*1*
2021	-	-
2020	*1*	-
2019	*1*	-
2018	-	-

Stadsbyggnadsnämnden		
2023	**-**	**-**
2022	-	-
2021	*1*	-
2020	-	-
2019	*1*	-
2018	-	-
Lantmäterinämnden		
2023	**-**	**-**
2022	-	-
2021	-	-
2020	-	-
2019	-	-
2018	-	-
Överförmyndarnämnden		
2023	**-**	**-**
2022	-	-
2021	-	-
2020	-	-
2019	-	-
2018	-	-
Södra Roslagens miljö- och hälsoskyddsnämnd		
2023	**-**	**-**
2022	*2*	-
2021	-	-
2020	*1*	-
2019	-	-
2018	-	*1*
Valnämnden		
2023	**-**	**-**
2022		
2021	-	-
2020	-	-
2019	-	-
2018	-	-
Äldrenämnden		
2023	***3***	-