Dataskyddsombudets årsrapport 2024 för barn- och grundskolenämnden

Juridikenheten
Ulrika Eek Eberharter
2025-03-10
Dnr BGN 2025/8-19

Innehållsförteckning

1. Inledning

I Täby kommuns verksamheter hanteras dagligen en stor mängd personuppgifter. Det centrala regelverket på området är EU:s dataskyddsförordning[1] (GDPR). Av förordningen framgår att dataskyddsombudet ska rapportera om dataskyddsarbetet direkt till den personuppgiftsansvariges högsta förvaltningsnivå, vilket huvudsakligen sker genom denna årsrapport.[2]

Personuppgifter är ett brett begrepp som omfattar all information som direkt eller indirekt kan härledas till en fysisk person i livet, såsom namn, personnummer, hälsouppgifter och fotografier. *Behandling* innebär t.ex. insamling, lagring och radering.

Den *personuppgiftsansvarige* styr över varför och hur personuppgifter ska behandlas och har det yttersta ansvaret. I kommunal organisation är det varje nämnd och bolag som är personuppgiftsansvarig inom sin respektive verksamhet. Inte kommunen som juridisk person. Personuppgiftsansvaret kan inte heller delegeras till enskild tjänsteman, även om det är denne som i praktiken arbetar med dataskyddsfrågorna.

Under året har dataskyddsombud, dataskyddsamordnare, cybersäkerhetsstrateg och informationssäkerhetssamordnare arbetat nära varandra. Även systemadministratör har bistått. På varje enhet ska det även finnas personer utsedda att stödja på enhetsnivå. Låg bemanning i kombination med personalomsättning under slutet av år 2024 försvårade dataskyddsarbetet, i synnerhet det proaktiva arbetet.

Denna rapport beskriver huvuddragen av det dataskyddsarbete som har utförts under det gångna verksamhetsåret 2024.

2. Registrerades rättigheter

3.1 Bakgrund

Dataskyddsförordningen ger de registrerade ett antal rättigheter, vilket är ett av huvudsyftena med förordningen.

[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.

Den registrerade har t.ex. rätt att få del av den information om denne som finns sparad hos kommunen (s.k. registerutdrag).[3] Vidare finns en rätt att få felaktiga personuppgifter korrigerade eller kompletterade (s.k. rätt till rättelse).[4] Det finns också en rätt att under vissa förutsättningar få sina personuppgifter raderade (s.k. rätt till radering).[5]

Dataskyddombudet är de registrerades kontakt i frågor som gäller kommunens hantering av personuppgifter. Under året har dataskyddsombudet besvarat frågor från allmänheten såväl som hanterat synpunkter och klagomål.

3.2 Statistik registerutdrag, rättelser och radering

Under året har totalt 25 stycken ärenden inkommit via e-tjänsten för personuppgiftshantering. Av dessa ärenden var 3 regelrätta begäran om registerutdrag och 2 ärenden regelrätta begäran om att rätta, begränsa eller radera personuppgifter. Övriga inkomna ärenden rörde andra frågor som t.ex. ansökan om förskoleplats eller begäran om allmän handling.

Tabell nr 1. Registerutdrag, rättning och radering 2018–2024

År	Antal begäran om registerutdrag	Antal begäran om rättelse	Antal begäran om radering
2024	**3**	**1**	**1**
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

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

personuppgifter. Brister i hanteringen kan även leda till tillsynsärenden från Integritetsskyddsmyndigheten (IMY) med sanktioner som följd. Numera finns även en rätt att överklaga IMY:s beslut, vilket innebär att den registrerades rättigheter har stärkts.[6] Ingen av kommunens nämnder eller bolag har varit föremål för IMY:s 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 är ett ständigt pågående arbete att effektivisera processen och att föra dialog med verksamheternas kontaktpersoner som på uppdrag av dataskyddssamordnare hanterar begäran om registerutdrag.

4. Incidenthantering

4.1 Bakgrund

Av dataskyddsförordningen följer en skyldighet att rapportera vissa personuppgiftsincidenter till IMY inom 72 timmar. Alla incidenter är inte rapporteringspliktiga, men samtliga incidenter måste dokumenteras internt.[7]

En incident kan vara vardagliga händelser, som en borttappad telefon, eller mer dramatiska händelser, som stora hackerattacker mot den centrala IT-miljön. Dataskyddförordningens definition av personuppgiftsincident är: ”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.”[8] Det spelar ingen roll om incidenten har skett oavsiktligt eller med avsikt.

Incidenthanteringen, som är både tidskritisk och ofta svårbedömd, sker i samarbete mellan berörd verksamhet och dataskyddsorganisationen. Stöd för anmälan av personuppgiftsincidenter finns på Insidan.

[6] HFD mål nr 6193-22, HFD mål nr 3691-22.
[7] Art. 33 dataskyddsförordningen.
[8] Art. 4.12 dataskyddsförordningen.

4.2 Statistik personuppgiftsincidenter

Under 2024 har totalt 32 personuppgiftsincidenter dokumenterats för kommunens samtliga nämnder. Tio av dessa har rapporterats vidare till IMY (p.g.a. dess allvarlighetsgrad). Ingen rapporterad incident har resulterat i att IMY har inlett ett tillsynsärende.

Tabell nr 2. Dokumenterade och rapporterade personuppgiftsincidenter 2018–2024

År	Incidenter – internt dokumenterade	Incidenter – rapporterade till IMY
2024	**22**	**10**
2023	34	1
2022	18	10
2021	15	4
2020	14	5
2019	22	3
2018	-	5

Fördelningen per nämnd finns i bilaga 1 till denna rapport.

4.3 Riskbedömning

Personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan dels leda till sanktionsavgifter, dels förtroendeskada för kommunen.

Det är fundamentalt att samtliga medarbetare kan identifiera en personuppgiftsincident och vet hur de ska agera redan vid *misstanke* om en sådan. Dataskyddombudet vill belysa det *dokumentationskrav* som finns för samtliga incidenter. Enligt dataskyddsförordningen ska samtliga personuppgiftsincidenter dokumenteras, oavsett om incidenten ska rapporteras till IMY eller inte.

Rutinen för incidenter 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.

Dataskyddsombudet vill understryka att ett högt antal rapporterade incidenter kan förklaras med en god förmåga att identifiera incidenter.

5. Övrigt dataskyddsarbete i urval

5.1 Internkontroll

5.1.1 Bakgrund

Dataskyddsorganisationen har under året genomfört två interna kontroller avseende kommunens förmåga att upprätta personuppgiftsbiträdesavtal. Detta med utgångpunkt i en risk fastställd i kommunstyrelsens interna kontrollplan för 2024. Rapporterna från granskningarna återfinns under dnr KS 2024/114-09.

Personuppgiftsbiträdesavtal behövs när personuppgiftshantering förekommer i avtalsrelationen och ett personuppgiftsbiträde (främst leverantörer) behandlar personuppgifter för en personuppgiftsansvarigs (nämnds) räkning. Att inte ingå ett sådant avtal när detta behövs, eller att använda ett som inte uppfyller dataskyddsförordningens krav på innehåll, strider mot förordningen och innebär onödiga risker för både den personuppgiftsansvarige och personuppgiftsbiträdet.

Under perioden 1 januari - 18 december 2024 har 208 stycken nyanskaffade/förnyade avtal registrerats i Täby kommuns avtalskatalog. Av dessa krävde 62 avtal närmare granskning för att avgöra dess relevans för aktuell kontrollpunkt. Totalt 9 av dessa avtal innehöll sådan personuppgiftshantering som kräver ett personuppgiftsbiträdesavtal. Av dessa avtal saknades personuppgiftsbiträdesavtal i 3 fall.

5.2.2 Riskbedömning

Kommunens förbättringsarbete ligger i att få alla verksamheter att arbeta med dataskyddskrav vid inköp/upphandling och att arbeta systematiskt med avtalsuppföljning. Centralt stöd i att ta fram avtalet finns och huvudavtalet kan inte anses giltigt innan personuppgiftsbiträdesavtal är upprättat.

5.2 Interna utbildningar

5.2.1 Bakgrund

Utbildning är den enskilt viktigaste insatsen för att reducera antalet personuppgiftsincidenter.

På Insidan presenteras, den för alla obligatoriska, webbutbildningen i dataskydd. Särskilda utbildningsinsatser har även genomförts, såväl för hela verksamhetsområden

som vissa specifika funktioner inom kommunen. Riktade utbildningar har efterfrågats av flera verksamheter, vilket dataskyddombudet upplever positivt.

5.2.2 Riskbedömning

Det är viktigt att arbetet med att utbilda all personal fortgår. Dataskyddsorganisationen kommer fortsatt att tillhandahålla webbaserad utbildning samt riktade utbildningar på förfrågan eller vid identifierat behov.

Varje enhet inom kommunen som hanterar personuppgifter i någon form bör även 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 den personuppgiftsansvarige skyldig att föra ett register över behandlingar som utförts under dess ansvar, en s.k. registerförteckning.[9] Det är en central förteckning eftersom den ger en överblick och kontroll av kommunens personuppgiftsbehandlingar. Förteckningen syftar till stor del till att alla verksamheter ska få förståelse för vilka personuppgifter som behandlas, samt att säkerställa att man faktiskt har rättslig grund för detta. Under 2024 fortlöpte arbetet med att kontrollera befintliga behandlingarna i registret (totalt omkring 600 stycken).

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.

Det är också viktigt att registret ses över med jämna intervaller samt vid behov.

5.4 Konsekvensbedömningar

5.4.1 Bakgrund

En konsekvensbedömning måste enligt dataskyddförordningen genomföras för personuppgiftsbehandlingar som kan medföra en hög risk för personuppgifterna, det

[9] Art. 30 dataskyddsförordningen.

vill säga en risk för de registrerades rättigheter och friheter.[10] Konsekvensbedömningar är ett viktigt kontrollverktyg vad gäller uppfyllnad av kraven i dataskyddsförordningen.

5.4.2 Riskbedömning

Kraven på konsekvensbedömningar är höga och kräver kunskap och engagemang från verksamheten. Frånvaro av eller bristfälliga konsekvensbedömningar kan leda till höga sanktionsavgifter och skadestånd.

Dataskyddsombudet anser att det är viktigt att kunskap finns om när en konsekvensbedömning behöver genomföras så att dataskyddsorganisationen kan involveras i tid. Det är även viktigt att bedömningen följs upp och uppdateras vid behov.

5.5 Överföring till tredjeland

5.5.1 Bakgrund

Tredjelandsöverföringar är när personuppgifter skickas eller på annat sätt görs tillgängliga för en mottagare i ett land utanför EU/EES-området, vilket t.ex. sker vid användandet av amerikanska molntjänster. Sådana överföringar är endast tillåtna under vissa förutsättningar. Det är exempelvis tillåtet att överföra personuppgifter till länder som EU-kommissionen har godkänt genom ett beslut om s.k. ”adekvat skyddsnivå”.

Sedan 2023 finns ett beslut om adekvat skyddsnivå för USA, det s.k. ”EU-U.S. Data Privacy Framework”. Beslutet är baserat på en överenskommelse mellan EU och USA om hur personuppgifter som överförs från EU- och EES-länderna ska skyddas i USA.

5.5.2 Riskbedömning

USA:s nuvarande administration anses äventyra EU-US Data Privacy Framework. Dataskyddsorganisation kommer fortsätta att följa händelseutvecklingen och stötta verksamhetsrepresentanter i diskussionen om lämpligheten att upprätta avtal med leverantörer där personuppgifter kan komma att lagras i tjänster i tredjeland.

[10] Art. 35 dataskyddförordningen.

Bilaga 1. Incidentstatistik

Personuppgiftsincidenter per nämnd 2018–2024

Personuppgiftsansvarig nämnd	Årtal	Incidenter internt dokumenterade	Incidenter rapporterade till IMY
Kommunstyrelsen	**2024**	**4**	**3**
	2023	2	-
	2022	-	-
	2021	3	-
	2020	-	-
	2019	8	1
	2018	-	-
Kultur- och fritidsnämnden	**2024**	**-**	**-**
	2023	2	-
	2022	-	2
	2021	1	-
	2020	-	1
	2019	-	-
	2018	-	1
Socialnämnden	**2024**	**9**	**3**
	2023	22	-
	2022	11	3
	2021	8	3
	2020	12	4
	2019	7	-
	2018	-	1
Barn- och grundskolenämnden	**2024**	**5**	**1**[11]
	2023	3	-
	2022	2	4
	2021	2	1
	2020	-	1
	2019	7	1
	2018	-	2
Gymnasie- och näringslivsnämnden	**2024**	**-**	**1**
	2023	1	1

[11] Detta är samma incident som finns noterad för gymnasie- och näringslivsnämnden för 2024.

Personuppgiftsansvarig nämnd	Årtal	Incidenter internt dokumenterade	Incidenter rapporterade till IMY
	2022	3	1
	2021	-	-
	2020	1	-
	2019	1	-
	2018	-	-
Stadsbyggnadsnämnden	**2024**	**-**	**-**
	2023	-	-
	2022	-	-
	2021	1	-
	2020	-	-
	2019	1	-
	2018	-	-
Lantmäterinämnden	**2024**	**-**	**-**
	2023	-	-
	2022	-	-
	2021	-	-
	2020	-	-
	2019	-	-
	2018	-	-
Överförmyndarnämnden	**2024**	**-**	**2**
	2023	-	-
	2022	-	-
	2021	-	-
	2020	-	-
	2019	-	-
	2018	-	-
Södra Roslagens miljö- och hälsoskyddsnämnd	**2024**	**-**	**-**
	2023	-	-
	2022	2	-
	2021	-	-
	2020	1	-
	2019	-	-
	2018	-	1
Valnämnden	**2024**	**1**	**-**
	2023	-	-
	2022		

Personuppgiftsansvarig nämnd	Årtal	Incidenter internt dokumenterade	Incidenter rapporterade till IMY
	2021	-	-
	2020	-	-
	2019	-	-
	2018	-	-
Äldrenämnden	**2024**	**3**	**1**
	2023	3	-