Mottagare
Socialnämnden

GDPR rapportering och uppföljning

Förslag till beslut
Socialnämnden godkänner informationen.

Sammanfattning
I denna rapportering redogörs för förvaltningens aktuella frågor avseende GDPR samt statistik för inkomna begäran om registerutdrag, raderingar och rättelse samt inträffade personuppgiftsincidenter sedan förra rapporteringen i februari 2025.

Dataskyddsombudet har under år 2025 genomfört tillsynsaktiviteter inom områden som laglighet för behandling av personuppgifter, behandling av uppgifter som rör barn, processorienterad dokumentation av personuppgiftsbehandling, behandling av personuppgifter med artificiell intelligens (AI) och en årlig uppföljning av molntjänster. Information ges om detta och förvaltningens svar.

Ärendebeskrivning
I denna rapportering redogörs för förvaltningens aktuella frågor avseende GDPR samt statistik för inkomna begäran om registerutdrag, raderingar och rättelse samt inträffade personuppgiftsincidenter sedan förra rapporteringen i februari 2025.

Personuppgiftsincidenter
En personuppgiftsincident är en säkerhetsincident som uppkommer då människors friheter eller rättigheter hotas. Detta sker till exempel när personuppgifter har hamnat i fel händer, blivit förstörda eller tappats bort; oavsiktligt eller med avsikt. En personuppgiftsincident ska anmälas till kontaktpersonerna för GDPR- frågor som därefter, oftast i samråd med dataskyddsombudet, bedömer om en anmälan ska göras till Integritetsskyddsmyndigheten (IMY). En sådan anmälan ska göras inom 72 timmar efter upptäckt incident.

Under år 2025 har det inträffat 18 personuppgiftsincidenter som anmälts vidare till IMY. Beslut har kommit från IMY i sex av fallen och IMY har i alla dessa fall beslutat att lägga ner ärendet.

	År 2025	År 2024	År 2023	År 2022
Antal personuppgifts-incidenter anmälda till IMY	18	20	8	11

Vid genomgång av incidenter som rapporterats till IMY under året framkommer i huvudsak följande orsaker till incidenter:

- Obehörigt röjande genom felaktigt utskick av mejl/brev/sms
- Obehörigt röjande: övrigt

Det vanligaste är att mottagaradressen blivit fel och att utskicket därför nått en annan mottagare än den som var avsedd. Obehörigt röjande: övrigt, har främst rört tillfällen då exempelvis namn på brukare har funnits i ett mejl som förvisso gått till rätt mottagare men där utskicket gjorts via vanlig mejl (till skillnad från säkra meddelanden) och till extern part (person som inte har en @gotland.se-adress). Informationen i mejlet bedöms då sakna skydd, och även om det inte finns något som tyder på att en obehörig tagit del av informationen så går det inte heller att utesluta att så skett eller kan komma att ske och anmälan har därför gjorts till IMY.

Regionen har tidigare inte behövt anmäla till IMY när mejl med personuppgifter skickats internt inom regionen. Det eftersom informationen i mejlet då inte lämnade de egna servrarna. I och med införandet av Microsoft 356 är all mejlkorrespondens kopplad mot Microsofts moln och numera behöver även situationer där personuppgifter förekommer i intern mejlväxling via Outlook anmälas som en personuppgiftsincident till IMY.

Tidigare har en mer ofta förekommande incident handlat om incidenter i samband med utskrifter. Exempelvis att dokument skrivits ut på fel skrivare eller att utskrift har legat kvar i skrivaren och att annan person tagit del av den. Region Gotland har, med start under sommaren 2025, infört något som kallas follow-me-print, vilket betyder att medarbetare kan skriva ut och hämta sina utskrifter på ett säkert sätt (med identifikation) på vilken skrivare man vill. Inget skrivs ut utan att personen själv befinner sig vid skrivaren och aktivt gör en utskrift. Detta bedöms i princip kunna bidra till att sådana incidenter inte längre kommer att inträffa.

<u>Begäran om registerutdrag, rättelse och radering</u>
Enligt GDPR har alla rätt att begära ett utdrag av de personuppgifter som Region Gotland har om en själv. En person har även rätt att begära rättelse eller en korrigering av personuppgifter som är felaktiga, ofullständiga eller oriktiga respektive rätt att begära radering av personuppgifter, dock med undantag av de personuppgifter som Region Gotland måste spara med stöd av exempelvis Offentlighets- och sekretesslagen (2009:400) och Arkivlagen (1990:782).

Totalt antal inkomna begäran om registerutdrag, rättelse och radering:

	År 2025	År 2024	År 2023	År 2022
Begäran om registerutdrag	12	11	17	6
Begäran om rättelse	0	1	0	0
Begäran om radering	0	1	0	0

Tillsynsaktiviteter av dataskyddsombudet
Dataskyddsombudet har under år 2025 genomfört tillsynsaktiviteter enligt följande:

- Laglighet för behandling av personuppgifter, förekommer behandlingar utan rättslig grund?
- Behandling av uppgifter som rör barn, rättsliga grunder, skydd och fullgörande av skyldigheter mot dem…..
- Processorienterad dokumentation av personuppgiftsbehandling, LISa - kompletterande redovisning där mer än ett system används för behandling utifrån ett ändamål och syfte med behandlingen
- Behandling av personuppgifter med AI
- Årlig uppföljning av molntjänster, insamling och inventering av villkor

Förvaltningen har lämnat svar på samtliga frågor och fullständiga svar för tillsynsaktiviteterna finns att hitta som bilagor till denna skrivelse. Dataskyddsombudet har ännu inte lämnat någon rapport utifrån regionens svar på tillsynen, det väntas komma under våren 2026.

Här följer en sammanfattning av förvaltningens svar:

1. **Laglighet för behandling av personuppgifter, förekommer behandlingar utan rättslig grund?**

Den som är personuppgiftsansvarig, i det här fallet socialförvaltningen, behöver ha en rättslig grund utifrån GDPR för behandling av personuppgifter. De system eller tjänster som används för behandling av personuppgifter genomgår en klassning och det är i samband med denna som rättslig grund för behandlingen anges.

För att svara på fråga nummer ett i dataskyddsombudets tillsynsaktiviteter så har genomgång gjorts av de totalt 54 klassningar som fanns inom förvaltningen vid svarstillfället. Genomgången visade att det inte förekom behandling utan rättslig grund, men att det i vissa fall behövdes göras ny bedömning om den rättsliga grunden skulle vara annan än den som angetts vid klassningstillfället. Skälet till att några av de rättsliga grunderna som angivits inte bedömdes stämma är troligtvis att förståelsen och kunskapen gällande de kriterier som behöver uppfyllas för val av rättslig grund med tiden har ökat i förvaltningen, vilket lett till att det nu finns andra förutsättningar för bedömning av rättslig grund.

Efter genomgången har ändring gjorts till rätt rättslig grund i samtliga klassningar där det bedömdes finnas behov av det.

2. Behandling av uppgifter som rör barn, rättsliga grunder, skydd och fullgörande av skyldigheter mot dem.

Personuppgifter som tillhör barn är enligt dataskyddsförordningen *särskilt skyddsvärda* och kräver extra försiktighet och högre skyddsnivåer än vuxnas uppgifter, eftersom barn är mer sårbara och har svårare att förstå riskerna med datadelning.

Efter genomgång av de system och tjänster som behandlar personuppgifter gällande barn framgår att det inte förekommer några särskilda skyddsåtgärder vid hantering av dessa personuppgifter. Då barn utgör en väntad del av socialförvaltningens målgrupp så har de verksamhetssystem som används vid behandlingen av deras personuppgifter bedömts uppfylla säkerhetskraven i sin helhet. Även vuxna individers personuppgifter har i dessa system ett starkt skydd utifrån sekretess och verksamheternas känsliga karaktär.

Förvaltningen ser dock att det finns behov av att ta fram lättförståelig information om GDPR riktad till barn.

3. Processorienterad dokumentation av personuppgiftsbehandling, LISa, kompletterande redovisning där mer än ett system används för behandling utifrån ett ändamål och syfte med behandlingen.

Dataskyddsombudets tillsynsaktivitet nummer tre handlar om behovet av att tydligare dokumentera hur personuppgifter behandlas i regionens processer, särskilt när flera IT-system och externa parter används. Förvaltningen uppmanas att identifiera de processer där flera system eller externa parter ingår och sedan komplettera dokumentationen för dessa.

I svaret till dataskyddsombudet anges att förvaltningen är medveten om behovet av att kunna redovisa personuppgiftsbehandling utifrån de registrerades perspektiv. Det vill säga, utifrån perspektivet hos dem vars personuppgifter som behandlas. Det rör bland annat möjligheten att kunna få ut fullständiga så kallade registerutdrag, där den enskilde har rätt att få en sammanställning av hur, var och varför dennes personuppgifter behandlas av förvaltningen.

Förvaltningen har ett pågående arbete kring hur dokumentationen av personuppgiftsbehandlingen kan bli mer processorienterad. Ett alternativ som ses över är att klassningar får en ny benämning. Exempelvis att *Klassning för Lifecare* i stället namnges som *Klassning Process dokumentation för behandling och insatser för socialtjänsten (Lifecare)*. I samband med att benämningen ses över skulle även själva processen förtydligas i klassningen. Förvaltningen har som mål att vara klar med arbetet i april 2026.

Förvaltningen ser dock även behov av ett regionövergripande arbete för att förenkla den information som medborgare får när de vänder sig till regionen för att få underrättelse om hur deras personuppgifter behandlas.

4. Behandling av personuppgifter med AI.

Tillsynsaktivitet nummer 4 handlar om att kartlägga hur AI används för att behandla personuppgifter inom förvaltningen. Syftet är att identifiera risker och behov av skyddsåtgärder.

Inom socialförvaltningen uppges det inte förekomma behandling av personuppgifter med AI så frågorna i tillsynsaktivitet nummer 4 har inte varit aktuella för förvaltningen att ge ett mer utförligt svar på.

5. Årlig uppföljning av molntjänster, insamling och inventering av villkor.

En molntjänst är en digital tjänst som nås via internet. Lagring eller system finns på internet i stället för på den egna datorn eller servern.

Några av förvaltningens upphandlade system och processer är molntjänster, till exempel trygghetslarm för personer i ordinärt boende och träningsprogram för personer som har hemsjukvård. Det förekommer även molntjänster som socialförvaltningen använder men som förvaltas av annan förvaltning, till exempel HR- och ekonomisystem. Det finns också molntjänster där socialförvaltningen som offentlig myndighet förväntas att rapportera in personuppgifter, till exempel till Socialstyrelsen. Molntjänster kan även användas av medarbetare för egen förkovran, information eller utbildning inom sitt yrkesområde, till exempel samarbetsforum hos SKR (Sveriges Kommuner och Regioner) och Dela Digitalt (en portal för samverkan, erfarenhetsutbyte, samfinansiering och gemensam verksamhetsutveckling inom offentlig sektor).

Molntjänsterna som förvaltningen använder har i svaret till dataskyddsombudet listats i tabeller och det har också angivits om det finns PUB-avtal (personuppgiftsbiträdesavtal) eller inte. Socialförvaltningen gör årligen en uppdaterad sammanställning över de molntjänster som förvaltningen använder.

<u>Övrigt aktuellt inom området</u>

- Förvaltningen gör ett arbete med att se över hur de ska hantera inkomna begäran om kontaktuppgifter till flertalet medarbetare. Förvaltningen har ett ansvar för hur personuppgifter hanteras efter utlämnande. I takt med att efterfrågan på kontaktuppgifter har ökat och att även hot och våld mot tjänstepersoner ökar är det här en angelägen fråga. Arbete pågår.

- Under 2025 har Region Gotland infört Microsoft 365 som standardplattform. Detta har medfört att frågor rörande informationssäkerhet blivit än mer framträdande och alla behöver bli bättre på hur information och känsliga uppgifter ska hanteras. Alla användare, både tjänstepersoner och förtroendevalda, har därför ombetts att genomgå informationssäkerhetsutbildning. Alla som inte genomgått utbildningen uppmanas att göra det snarast. Utbildningarna (en från Region Gotland och en från Myndigheten för samhällsskydd och beredskap) finns i Kompetensportalen som hittas i Portalen. Fråga någon av nämndsekreterarna om hjälp om ni ännu inte genomgått dessa utbildningar.

  Vi påminner också om att e-post som innehåller känslig information eller personuppgifter inte får hanteras i vanlig e-post eftersom det då lagras i molnet. Nämnden/förvaltningen kan inte ta ansvar för vad som inkommer i e-posten men ansvar måste tas för vidare hantering av informationen. E-posten får inte vidarebefordras till annan eller besvaras i vanlig e-post utan endast via säkra meddelanden. .

Bedömning

Socialnämnden föreslås godkänna rapporten angående GDPR.

Beslutsunderlag

Tjänsteskrivelse, daterad 2024-01-11.
Dataskyddsombudets tillsynsaktiviteter 2025, SON 2025/375:1 (sekretess)
Delegationsbeslut gällande tillsynsaktivitet nr 1, SON 2025/375:2 (sekretess)
Delegationsbeslut gällande tillsynsaktivitet nr 2, SON 2025/375:7 (sekretess)
Delegationsbeslut gällande tillsynsaktivitet nr 3, SON 2025/375:9 (sekretess)
Delegationsbeslut gällande tillsynsaktivitet nr 4, SON 2025/375:12 (sekretess)
Delegationsbeslut gällande tillsynsaktivitet nr 5, SON 2025/375:14 (sekretess)

Socialförvaltningen

Marica Gardell
Socialdirektör

Skickas till

Dataskyddsombud
Kontaktpersoner GDPR, socialförvaltningen