Mottagare
Socialnämnden

Tillsyn av personuppgiftsansvaret enligt den Europeiska Dataskyddsförordningen (GDPR) 2022

Förslag till beslut
Socialnämnden godkänner informationen.

Sammanfattning
Region Gotlands dataskyddsombud granskar årligen hur de personuppgiftsansvariga nämnderna inom Region Gotland behandlar personuppgifter för att säkerställa att behandlingen följer gällande regler samt att de registrerades integritet skyddas. Under år 2022 har följande områden granskats:

- Uppföljning av PUB-/samordningsavtal när behandling av uppgifter sker av annan än den personuppgiftsansvarige
- Information avseende personuppgiftsbehandling vid insamling av uppgifter
- Inventering kameraövervakning
- Uppföljning av dokumentation över behandlingar

Socialnämnden har inkommit med svar på samtliga frågor ovan (delsvaren har delgetts socialnämnden) och dataskyddsombudet har sammanställt en rapport över tillsynen till varje nämnd med förslag på åtgärder och rekommendationer.

Dataskyddsombudets bedömer att socialnämnden inte fullt ut uppfyller kraven i den Europeiska dataskyddsförordningen (GDPR). Bristerna anses bestå i bristande dokumentation, information och uppföljning. Det bedöms dock inte föreligga risk för att nämndens behandling av de registrerades personuppgifter äventyrar de registrerades personliga integritet. För att förbättra regelefterlevnaden till GDPR bör informationen till de registrerade samt instruktionerna avseende samordnat personuppgiftsansvar och personuppgiftsbiträden ses över och utvecklas.

De flesta åtgärdsförslagen och rekommendationerna i rapporten är sådana som både dataskyddsombudet och förvaltningen föreslår ska arbetas med regiongemensamt. Vissa är dock av den art att det är förvaltningen själva som bör arbeta med.

Ärendebeskrivning

Dataskyddsombudets rapport för granskningen 2022 innehåller en beskrivning av de fyra delområdena, en sammanfattning av förvaltningen svar samt en bedömning från dataskyddsombudet. Sammanfattningsvis finns ytterligare rekommendationer från dataskyddsombudet avseende nämndernas arbete med GDPR.

Efter att rapporten kom från dataskyddsombudet har diskussion lyfts i regionens GDPR-nätverk om att det är svårt att avgöra vilka åtgärder/rekommendationer som är bra om de handhas regionövergripande respektive hanteras i nämnderna var och en för sig. Dataskyddsombudet har därför gett ytterligare en rekommendation till regionen om hur en sådan uppdelning skulle kunna se ut. GDPR-nätverket kommer att gå igenom detta förslag gemensamt för att se över hur ansvarsfördelningen bör se ut.

I denna tjänsteskrivelse anges i texten ofta två system, LISA och W3D3, därför ges här en förklaring till dessa. LISA står för *Ledningssystem för InformationsSäkerhet Administration* och är verksamheternas IT-stöd för arbete med informationssäkerhet, dataskydd och förvaltning av IT-system. W3D3 är regionens diarieförings- och ärendehanteringssystem. Utgångspunkten är att nämndens alla allmänna handlingar i ärenden av långfristig betydelse ska hanteras i W3D3.

Informationsklassning är också ett begrepp som ofta nämns inom området GDPR och informationsförvaltning. Informationsklassning är en beskrivning/genomgång som görs av alla informationstillgångar och resurser som hanteras av regionen för att säkerställa att informationen ges nödvändigt skydd. I en informationsklassning svaras på frågor som vart informationen lagras, vilken information som hanteras, om GDPR gäller, vilken typ av personuppgifter som då hanteras, m m.

Delgranskning 1 – Uppföljning av PUB-/samordningsavtal när behandling av uppgifter sker av annan än den personuppgiftsansvarige

Personuppgiftsbiträdesavtal (PUB-avtal) är ett avtal mellan den personuppgiftsansvariga och ett personuppgiftsbiträde. Det reglerar hur biträdet får lov att hantera personuppgifter för den ansvariges räkning. PUB-avtalet är normalt en bilaga till affärsavtalet. Region Gotland har beslutat att PUB-avtal ska förvaras i systemet W3D3. I informationsklassningen (i LISA) ska man då även skriva in att det finns ett PUB-avtal och i vilket ärende i W3D3 som det kan återfinnas.

Socialförvaltningens avtalscontroller har hanterat denna delgranskning. Särskilt har granskning gjorts av åtta olika informationsklassningar (utifrån en bruttolista som dataskyddsombudet tagit fram) där dessa åtta innehåller personuppgifter som hanteras av extern part där biträdesavtal ska upprättas. Dessa har tittats på utifrån följande frågeställningar:

1. Finns PUB-avtal upprättat?
2. Är ärendenummer angivet i LISA?

3. Förvaras PUB-avtalet i W3D3?

Fyra av de kontrollerade posterna är godkända utan anmärkning. Två av de kontrollerade posterna är godkända med mindre anmärkning. En av dem hänvisar till ett felaktigt ärendenummer i diariesystemet W3D3, vilket behöver korrigeras. I ett fall behöver namnet på personuppgiftsbiträdet uppdateras i systemet LISA. Dessa anmärkningar har tagits till ansvariga för åtgärd. Slutligen är det två av de kontrollerade posterna som förvaltningen inte anser är godkända. I båda fallen anges det i LISA att det finns upprättat PUB-avtal, men det går inte att söka fram dessa i W3D3. Det är också återkopplat till ansvariga för åtgärd.

Vid en genomgång av alla förvaltningens informationsklassningar har dataskyddsombudet sett att det är femton objekt som saknar uppgifter om huruvida det finns PUB-avtal eller annat avtal. Förvaltningens avtalscontroller har gått igenom dessa och konstaterat att PUB-avtal inte behövs i något av dessa fall, de flesta av dem är dessutom lokala system. Förvaltningen kommer att föra in rätt uppgifter i LISA om detta.

För att förbättra arbetet rörande PUB-avtal, utifrån dataskyddsombudets bedömning och rekommendationer, ser förvaltningen att de initialt behöver göra följande:

- Identifiera de PUB-avtal som finns.
- Göra en plan för att gå igenom dessa och då börja med de äldsta först. Gå igenom instruktionerna i PUB-avtal för att säkerställa att de återspeglar hur den faktiska behandlingen och ansvarsfördelningen ser ut.
- Säkerställa att det finns en koppling mellan informationsklassningarna i systemet LISA och PUB-avtalen som lagras i systemet W3D3. Detta för att PUB-avtalen lätt ska kunna hittas.
- Säkerställa att det är lätt att hitta PUB-avtal i W3D3.

Delgranskning 2 - Information avseende personuppgiftsbehandling vid insamling av uppgifter

I GDPR finns den grundläggande principen om att den personuppgiftsansvarige ska vara transparent avseende behandlingen av personuppgifter. En förutsättning för att de registrerade ska kunna utöva sina rättigheter är att personuppgiftsansvariga underlättar de registrerades tillgång till korrekt och rättvisande information om behandlingen som görs av deras personuppgifter. Informationen ska ges när informationen samlas in/behandlingen startar. En av delgranskningarna bestod i att förvaltningen skull se över hur denna information ges.

Förvaltningen har undersökt hur information om personuppgiftsbehandlingen sker på till exempel blanketter, i e-tjänster och på webben. Förvaltningens bedömning är att olika åtgärder behöver vidtas för att säkerställa att de

registrerade får tillräcklig information. Den information som ges idag är av olika karaktär, allt ifrån mycket god information till att ingen information ges på t ex en blankett. Därför ser förvaltningen att åtgärder skulle behöva utföras i olika steg:

1. Informationssäkerhetssamordnaren på Region Gotland kommer att se över den generella informationen om personuppgiftsbehandling som ges på regionens webbplats. Arbetet pågår.
2. Socialförvaltningens kontaktpersoner för GDPR ser därefter över om socialförvaltningen behöver ha en egen generell information på sin egen förvaltningssida på webben.
3. Tydlig instruktion bör ges till alla förvaltningens chefer om vilken information som ska finnas avseende personuppgiftsbehandling i alla e-tjänster, på alla blanketter och dokument där uppgifter inhämtas.
4. Alla avdelningschefer ges i uppdrag att se över alla blanketter, dokument och e-tjänster där information inhämtas och vid behov komplettera detta.
5. Uppföljning görs av att e-tjänster, blanketter och dokument har tillräcklig information om personuppgiftsbehandling.

Dataskyddsombudet delar förvaltningens bedömning av vad som behöver åtgärdas.

Delgranskning 3 - Inventering kameraövervakning

Avsikten med denna delgranskning var att inventera vilken kameraövervakning som förekommer i socialförvaltningens verksamheter, vilka tillstånd som föreligger samt vilka villkor som är förknippade med detta. Förvaltningens översyn visade att socialförvaltningens verksamheter använder sig av 2 stycken kameror som faller under kravet om tillstånd från Integritetsskyddsmyndigheten (IMY). Dessa kameror finns vid två av individ- och familjeomsorgens verksamheter i form av porttelefoner. Tillstånd har beviljats av IMY för dessa.

Förvaltningen har nyligen lämnat in en ny ansökan till IMY om att byta placering på en av de befintliga kamerorna. I och med den nya receptionsbyggnaden hos individ- och familjeomsorgen har den befintliga kameran behövt flyttats på och då behövs ett nytt beslut/tillstånd. Förvaltningen väntar svar på ansökan och hoppas det ska komma snabbare denna gång då det är samma kamera, samma syfte och samma funktioner som den förra, bara en ny placering.

Dataskyddsombudet nämner även digital nattillsyn i sin bedömning av förvaltningens kameraövervakning och förvaltningen har pågående diskussion med dataskyddsombudet kring detta. Dataskyddsombudets frågor kommer att lyftas till verksamheten.

Delgranskning 4 - Uppföljning av dokumentation över behandlingar
Den här delgranskningen är en uppföljning av en av de granskningar som gjordes år 2020 och där alla nämnder fick kritik då dokumentationen av behandlingarna inte uppfyllde kraven i GDPR (artikel 30). LISA är det system som används för att göra informationsklassningar och dessa klassningar görs utifrån informationsmängder eller system. Det som GDPR uttrycker är dock att dokumentationen ska utgå från de registrerades perspektiv och beskrivas enligt processer. De registrerade ska t ex kunna se om behandlingen av deras personuppgifter i ett visst syfte (t ex på grund av en ansökan) sker över flera system/kanaler. D v s se varje behandling från början till slut. Detta uppfylls alltså inte av Region Gotland med nuvarande arbetssätt.

Diskussioner har förts om detta internt under en längre tid men ännu har inget annat arbetssätt presenterats övergripande för regionen. Socialförvaltningen har i olika omgångar själva försökt hitta ett annat arbetssätt men ser också att det finns ett värde i att hela regionen gör på samma sätt i denna fråga.

Nuvarande arbetssätt kring dokumentationen behöver förändras men det kommer att innebära en stor arbetsinsats. Detta arbete är inte heller isolerat utan hänger ihop med andra frågor rörande GDPR vilket också komplicerar. Socialförvaltningen är aktiva i frågan om att få till en förändring och därmed kunna skapa en tydlighet för de registrerade hur deras personuppgifter hanteras i olika processer.

Bedömning
De flesta av åtgärdsförslagen och rekommendationerna från dataskyddsombudet är sådan som både dataskyddsombud och förvaltning anser är regionövergripande. Dessa behöver diskuteras i regionens GDPR-nätverk för att bedöma hur arbetet ska gå till och vilka som ansvarar.

Vissa åtgärder är dock förvaltningens ansvar och de har presenterats i denna tjänsteskrivelse.

Förvaltningen föreslår socialnämnden att en återkoppling av arbetet sker på nämndens sammanträde i december 2023.

Beslutsunderlag
Tjänsteskrivelse, daterad 2023-05-15.
Rapport från dataskyddsombudet, Tillsyn av Socialnämndens personuppgiftsansvar enligt den Europeiska Dataskyddsförordningen (GDPR) 2022, daterad 2023-02-17.

Socialförvaltningen

Marica Gardell
Socialdirektör

Skickas till
Region Gotlands dataskyddsombud