DSO:s årsrapport 2022
Dnr SOCN-2023-00165

Personuppgiftsansvarig
Socialnämnden

Dataskyddsombudets årsrapport 2022

Dataskyddsombud
Hanna Virtanen

Datum 2023-05-15, reviderad 2023-05-29

Innehåll

Inledning

Dataskyddsförordningen (GDPR) reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Som personuppgift räknas all typ av information som kan kopplas till en fysisk person. Varje organisation, oavsett verksamhet, behandlar därmed personuppgifter i någon omfattning och måste därmed förhålla sig till dataskyddsförordningens regler.

Förordningen ställer en rad krav; från säker hantering av information, till kontroll över vilka personuppgifter som hanteras, var, varför och hur samt kontinuerlig utvärdering av risker för enskildas fri- och rättigheter. Det är nämnden som är personuppgiftsansvarig för den personuppgiftsbehandling som sker inom dess verksamhet och därmed ytterst ansvarig för att förordningens krav följs.

Granskningens omfattning och metod

Denna rapport sammanfattar socialnämndens efterlevnad av dataskyddsförordningen fördelat på nio områden. Områdena beskrivs närmare i rapporten nedan tillsammans med en beskrivning av vilken/vilka kontrollpunkter som ingått i årets granskning. Granskningen har inte omfattat samtliga krav som ställs på en personuppgiftsansvarig, utan enbart utvalda punkter inom de nio områdena. Bedömningen av nämndens efterlevnad har därmed enbart gjorts utifrån de kontrollpunkter som ingått i årets granskning.

Rapporten lämnas av nämndens dataskyddsombud. Dataskyddsombud är en roll som nämndens är skyldig att utse enligt dataskyddsförordningen och har i uppdrag att granska och rapportera om nämndens efterlevnad. Därutöver har dataskyddsombudet även i uppgift att ge råd och stöd om skyldigheter som följer av lagen samt fungera som kontaktpunkt gentemot enskilda och tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY). Denna rapport överlämnas till nämndens styrelse som en del av dataskyddsombudets uppdrag.

Nämndens efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas nämndens efterlevnad av dataskyddsförordningen inom nio områden. Områdena beskrivs under respektive rubrik nedan tillsammans med en sammanfattning.

1. Registrera personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska enligt artikel 30 i GDPR ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade[1], typer av personuppgifter och lagringstid framgår. Registerförteckningen är förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens då den anger vilka personuppgifter som behandlas, hur och varför.

[1] Registrerade = enskilda vars personuppgifter hanteras

Årets granskning omfattar huruvida nämndens personuppgiftsbehandlingar har registrerats och om innehållet i registerförteckningen motsvarar kraven i artikel 30 i GDPR.

Nämndens efterlevnad

Registerförteckningen bedöms vara komplett och följer kraven i GDPR.

2. Grundläggande principer

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i GDPR. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar också övriga krav på dataskydd. Principer handlar bland annat om att enbart behandla personuppgifter med en rättslig grund, inte behandla fler personuppgifter än vad som behövs för att visst syfte, iaktta proportionalitet, inte spara uppgifter längre än de behövs och hantera personuppgifterna med tillräcklig säkerhet.

Årets granskning omfattar huruvida nämnden bedöms beakta principerna i sitt dataskyddsarbete utifrån informationen i registerförteckningen och genomförda konsekvensbedömningar samt om medarbetare får utbildning i GDPR för att kunna hantera personuppgifter korrekt i sitt dagliga arbete.

Nämndens efterlevnad

Nämnden bedöms beakta principerna i stort utifrån den information som dataskyddsombudet tagit del av under granskningen. Medarbetare inom nämnden har fått utbildning i GDPR

3. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda och åtgärda personuppgiftsincidenter samt anmäla vissa incidenter till tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY). Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Det är även av vikt att incidenten leder till uppdaterade rutiner och arbetssätt för att förhindra nya incidenter.

Årets granskning omfattar huruvida nämnden utbildar medarbetare i incidenthanteringsprocessen och om enheter hanterar uppkomna incidenter i enlighet med kommunens gemensamma process för incidenthantering.

Nämndens efterlevnad

Nämnden följer den kommungemensamma processen för hantering av personuppgiftsincidenter. I samband med övrig GDPR-utbildning och efter incidenter har medarbetare informerats om incidenthanteringsprocessen och hur

framtida incidenter kan förhindras. Under 2022 rapporterades 23 st. incidenter in, varav 3 av dessa anmäldes vidare till tillsynsmyndigheten (IMY).

4. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning. Exempel på situationer då en hög risk kan föreligga är: övervakning eller kartläggning av personer i beroendesituation, behandling av känsliga personuppgifter eller användning av ny teknik. Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt för den personuppgiftsansvarige att visa att dataskyddslagstiftningen följs. Om en hög risk kvarstår efter en konsekvensbedömning ska dessutom tillsynsmyndigheten (IMY) kontaktas för ett förhandssamråd innan personuppgiftsbehandlingen påbörjas.

Årets granskning omfattar huruvida nämndens genomfört en riskbedömning för att bedöma om en konsekvensbedömning krävs och om konsekvensbedömningen därefter är gjord.

Nämndens efterlevnad

Dokumentation över vilka personuppgiftsbehandlingar som kräver en konsekvensbedömning saknas delvis. Konsekvensbedömningar är gjorda för delar av nämndens personuppgiftsbehandlingar.

5. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal (PUB-avtal) ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter åt den personuppgiftsansvariga. Den externa parten är då biträde till den personuppgiftsansvariga och ska genom PUB-avtalet förbindas att endast behandla personuppgifter efter instruktioner från den ansvarige. Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas även när det är någon annan än den personuppgiftsansvarige som behandlar personuppgifterna.

Årets granskning omfattar huruvida nämnden kartlagt sina externa parter för att säkerställa att PUB-avtal tecknas där så krävs.

Nämndens efterlevnad

Inom objektförvaltningen sker för närvarande en genomgång för att säkerställa att nödvändiga avtal, bland annat personuppgiftsbiträdesavtal (PUB-avtal) finns på plats. För upphandlingar som gjorts nyligen och nämndens verksamhetssystem har PUB-avtal tecknats med de parter som bedömts vara personuppgiftsbiträden och där nämnden ansvarar för systemförvaltningen. PUB-avtal saknas dock för system som delas med regionen, men ett arbete med att ta fram avtalet pågår med länets kommuner och regionen.

6. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast behandlas får behandlas så länge de behövs för ändamålet. Inom offentlig verksamhet innebär lagringsminimering att det finns ordning och reda bland myndighetens information och att styrdokument, en informationshanteringsplan (IHP), tagits fram som anger hur informationen ska hanteras och om den ska bevaras eller gallras.

Årets granskning omfattar om nämndens har en uppdaterad IHP och om arkivering och gallring utförs enligt den.

Nämndens efterlevnad

Informationshanteringsplaner finns beslutade från 2021 och 2022 (och en revidering är på gång). Arkivering och gallring sker enligt den beslutade IHP:n.

7. Registrerades rättigheter

Enskilda har ett antal rättigheter i förhållande till sina personuppgifter, nämligen:

- Rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”)
- Rätt att få information om hur personuppgifter hanteras (rätten till information)
- Under vissa förutsättningar få sina uppgifter raderade eller rättade (rätten till radering och rättelse)
- Rätt att invända, dvs. motsätta sig, mot en personuppgiftsbehandling och även begära begränsning av personuppgifternas användning (Rätten att göra invändningar och begära begränsning)
- Rätt att inte bli föremål för automatiskt beslutsfattande[2]
- Rätt att få ut sina personuppgifter på ett strukturerat sätt för att använda de hos någon annan (rätt till dataportabilitet – gäller enbart i få specifika fall inom offentlig förvaltning)

För att enskild ska kunna utöva sina rättigheter krävs att den personuppgiftsansvariga känner till rättigheterna och har rutiner för att ta hand om en begäran om att utöva något av rättigheterna. Rätten till information gäller dock utan att en enskild behöver begära detta särskilt, vilket betyder att en personuppgiftsansvarig måste säkerställa att information ges på ett tydligt och lättillgängligt sätt.

Årets granskning omfattar om nämnden har processer för att hantera registrerades rättigheter och om nämndens ger enskilda den information de har rätt till enligt kraven i dataskyddsförordningen.

[2] Beslut som fattas utan att en fysisk person är inblandad.

Nämndens efterlevnad

Varje nämnd följer den kommungemensamma processen för begäran av registerutdrag (rätten till tillgång). Under 2022 har registerutdrag på kommunnivå enbart vid några tillfällen hanterats i tid. Den överenskomna kommungemensamma processen följer inte heller helt kraven i GDPR då inga kopior av själva personuppgifterna lämnas vid den första begäran, utan den registrerade måste återkomma igen för att få ta del av dem. För socialnämndens del har svar lämnats i tid, men då den registrerade får ett gemensamt svar från alla nämnder som berörs av en begäran har svaret till den registrerade ändå skickats för sent (i de fall andra nämnder berörts av en begäran). Förändringar i den kommungemensamma processen har nyligen gjorts för att säkerställa att registerutdrag skickas inom de lagstadgade tidsramarna, men då inga kopior lämnas i första skedet följer hanteringen fortfarande inte GDPR i denna del.

Vad gäller information till registrerade (rätten till information) uppfylls inte kraven helt. GDPR innehåller både krav på vilken typ av information som ska lämnas och när detta ska ske. Om personuppgifter inhämtas direkt från en registrerad ska information lämnas i samband med att uppgifterna samlas in, exempelvis via ett formulär. Om personuppgifterna hämtas från någon annan källa ska information ges vid första kontakt. För socialnämndens del saknas tydlig och lättillgänglig information om hur nämnden behandlar registrerades personuppgifter.

Övriga rättigheter utövas sällan av registrerade, men medarbetare inom nämnden har kännedom om dem och hur de ska hanteras.

8. Känsliga och extra skyddsvärda personuppgifter

Det finns ett generellt förbud mot att hantera känsliga personuppgifter[3] i dataskyddsförordningen. Det är enbart tillåtet om en av undantagen är tillämpliga, därför är det viktigt att veta om eventuella känsliga personuppgifter som behandlas är laglig. Förutom känsliga personuppgifter, finns det en grupp personuppgifter kallat extra skyddsvärda[4] personuppgifter som inte kräver ett undantag för att det ska vara tillåtet att hantera dem, men är samtidigt av en karaktär som kräver att de skyddas med högre säkerhet. Dessa typer av uppgifter och känsliga personuppgifter får enbart hanteras enligt säkerskilda rutiner och i system/lagringsytor som har högre säkerhet.

Årets granskning omfattar huruvida nämndens bedöms ha rättslig grund (ett undantag) för behandling av sina känsliga personuppgifter och huruvida rutiner finns för hantering av känsliga och extra skyddsvärda personuppgifter.

---

3 För en beskrivning av känsliga personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter

4 För en beskrivning av extra skyddsvärda personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter

Nämndens efterlevnad

Det har inte framkommit att känsliga personuppgifter behandlas utan rättslig grund. Både känsliga och extra skyddsvärda personuppgifter hanteras enligt särskilda rutiner.

9. Informationssäkerhet

En av de grundläggande principerna är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). Med andra ord handlar det om att arbeta aktivt med informationssäkerhet.

Årets granskning omfattar huruvida nämnden har ett informationssäkerhetsarbete och genomför analyser kopplat till detta, exempelvis informationsklassning och riskanalys.

Nämndens efterlevnad

Informationsklassningar och riskanalyser har gjorts inför upphandlingar av nya system. Nämndens system ingår nu i kommunens modell för objektsstyrd systemförvaltning och inom objektet kommer informationssäkerhetsaktiviteter och -åtgärder att genomföras.

Sammanfattning av nämndens efterlevnad och dataskyddsombudets rekommendationer

Nämnden efterlever dataskyddsförordningen i princip alla delar, men inom några få områden krävs åtgärder för att uppfylla kraven i sin helhet. Dataskyddsombudet ger därför följande rekommendationer:

- Färdigställa konsekvensbedömningar (DPIA) för befintliga personuppgiftsbehandlingar, där så krävs.
- Säkra att personuppgiftsbiträdesavtal (PUB-avtal) tecknas, där så krävs, och rollerna i övrigt är klargjorda där nämndens personuppgifter behandlas av en annan part.
- Ge enskilda komplett och tydlig information om hanteringen av sina personuppgifter enligt dataskyddsförordningen krav.