NORRTÄLJE KOMMUN

2024-11-04
Dnr: XX

Årsrapport 2024 avseende dataskydd för Socialnämnden

Inledning

Dataskyddsförordningen (GDPR) reglerar hantering av personuppgifter, alltså allt som kan kopplas till en fysisk person.

Förordningen ställer en rad krav på verksamheten, från kontroll över vilka personuppgifter som hanteras, var, varför och hur, till säker hantering av information, samt kontinuerlig utvärdering av risker för enskildas fri- och rättigheter. Det är nämnden/bolaget som är personuppgiftsansvarig därmed ytterst ansvarig för att förordningens krav följs.

Dataskyddsombudet har som uppdrag att granska nämnders och bolags efterlevnad av dataskyddsförordningen.

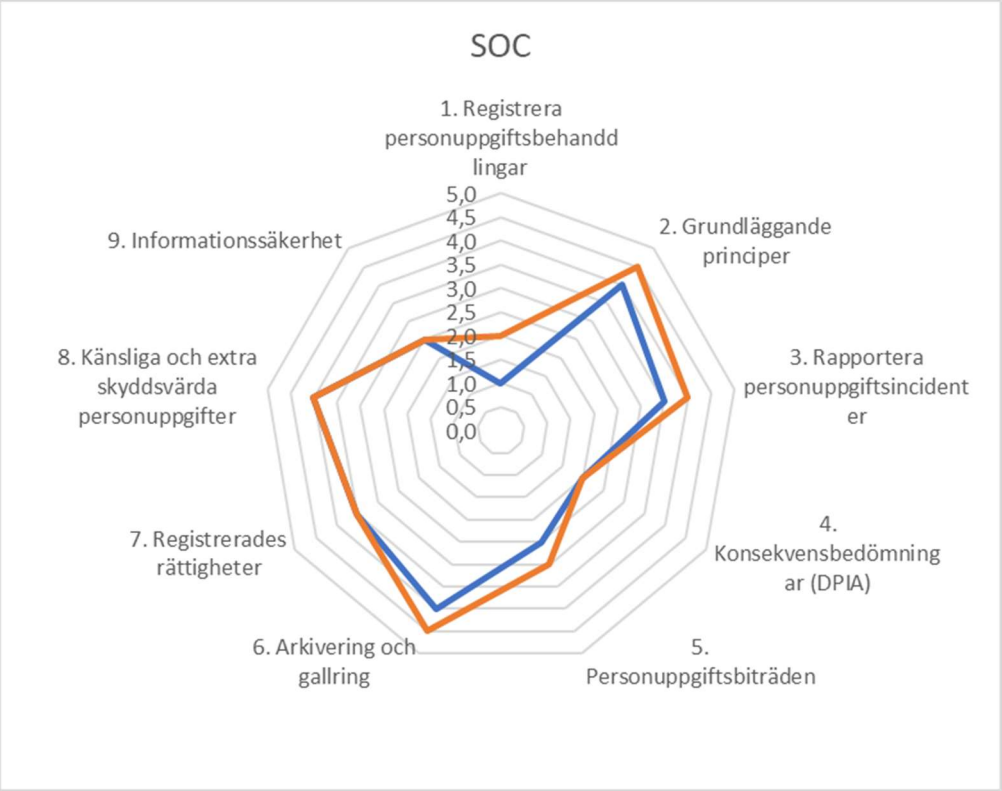
Syfte

Syftet med årsrapporten är att ge en bild av hur efterlevnaden av dataskyddsförordningen inom kommunen ser ut idag jämfört med föregående år, samt ge förbättringsförslag. Rapporten syftar även till att ge ledningen ett prioriterat angreppsätt för att stegvis förbättra efterlevnaden av reglerna samt följa upp utvecklingen.

Metod

Denna rapport delar in dataskyddsförordningen i nio delområden, dessa beskrivs i bilagan. Prioriterade delar inom varje område har granskats och inte helheten av varje del. Enkät och dialog har skett med utsedda kontaktpersoner inom verksamheterna. Därefter har uppskattning av regelefterlevnad gjorts inom respektive område där 0 är lägst och 5 är högsta nivån.

Status



Spindeldiagrammet visar status avseende efterlevnad av de nio delområdena inom socialnämnden. Blå: 2023 och Orange: 2024.

Utvärdering och prioritering

Utvärdering

Efter förra årets rapport har arbetet på central nivå prioriterat behandlingsregister, utbildningsinsatser och incidenthantering.

Behandlingsregistret har förbättrats och gått från system till behandlingar och nytt systemstöd är under implementering. Två utbildningar finns i mitt lärande, en grundkurs och en fördjupningskurs. Genomförandenivån av kurserna kan förbättras.

Incidenthanteringsprocessen har tagit mer tid än beräknat. Kommunen har behov av olika typer av incidentrapporteringar/avvikelser och förhoppningen är att hitta en lösning för alla incidentrapporteringar/avvikelser.

Uppdatering har skett på norrtalje.se med information om behandling av personuppgifter samt genomgång av e-tjänst för registerutdrag.

Senaste året har utvecklingen för dataskyddsarbete förbättrats eftersom kompetensen för informationssäkerhet har stärkts.

Socialnämndens arbete har inte haft önskad progress vad gäller behandlingsregistret på grund av resursbrist. Behandlingsregistret behöver uppdateras och kompletteras för att skapa förutsättningar att genomföra konsekvensbedömningar som krävs enligt lagstiftning. Verksamheten har under året uppdaterat hanteringsanvisningarna och dessa underlättar arbetet med behandlingsregistret.

Årsrapporten med egenkontrollerna tas emot av verksamheten som ett bra verktyg för att prioritera åtgärder.

Prioriterade åtgärdsförlag

- Kommunens behandlingsregister (artikel 30 registret):
    - Uppdatera och komplettera behandlingsregistret för socialnämnden
    - Implementera nya systemstödet för behandlingsregistret
    - Ta fram metodstöd för genomförande av konsekvensbedömningar
    - Utvärdera behov konsekvensbedömningar i verksamheten
    - Behandlingar mellan nämnder och behandlingar mellan nämnder och kommunala bolag behöver skriftligen regleras
- Ny rutin för rapportering av personuppgiftsincidenter:
    - Lättare för verksamheterna att rapportera, vi har ett stort mörkertal
    - Tydlighet i vad som ska rapporteras och få medarbetarna att inte känna skuld i samband med en incident
    - Systematisk uppföljning för att upptäcka brister och bli bättre
- Ledningens aktiva arbete med dataskyddsfrågor i verksamheterna:
    - Avsätta resurser
    - Tillse att kompetens finns i verksamheten
    - Följa upp utvecklingen
- Informationssäkerhet:
    - Fortsätta förberedelser för kommande cybersäkerhetslag
    - Prioritera åtgärdsförslagen enligt cybersäkerhetskollen

Bilaga 1

Information om respektive punkt i egenkontrollen.

1. REGISTRERA PERSONUPPGIFTSBEHANDLINGAR

I detta avsnitt ställs två frågor enligt nedan:
1. Verksamhetens registerförteckning är komplett.
2. Informationen i registerförteckningen är aktuell.

En förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens regler är att veta vilka personuppgifter som behandlas och varför. Varje personuppgiftsansvarig (nämnd inom kommunal förvaltning) ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, typer av personuppgifter och lagringstid framgår.

I Norrtälje kommuns verksamheter registreras personuppgiftsbehandlingar i systemstödet. Detta görs oftast av en dataskyddssamordnare eller annan utsedd person i verksamheten.

2. GRUNDLÄGGANDE PRINCIPER

I detta avsnitt ställs tre frågor enligt nedan:
1. Verksamheten har kännedom om de grundläggande principer och dessa beaktas i verksamhetens arbete som rör personuppgifter
2. Verksamhetens medarbetare har genomfört grundläggande utbildning i GDPR
3. Verksamheten använder samtycke som rättslig grund enbart i situationer då kriteriet för frivillighet uppfylls

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar även övriga krav på dataskydd. Därför är det viktigt att känna till principerna och beakta dessa i frågor som rör personuppgifter. Det handlar bland annat om att ha en rättslig grund, enbart behandla så många personuppgifter som behövs för ett visst syfte, inte spara längre än de behövs och ha tillräcklig säkerhet.

De grundläggande principerna är:

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering

- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

3. RAPPORTERA PERSONUPPGIFTSINCIDENTER

I detta avsnitt ställs fyra frågor enligt nedan:
1. Verksamhetens medarbetare är informerade om definitionen och processen för personuppgiftsincidenter (på en introduktion, minst årligen på APT eller liknande)
2. Verksamhetens medarbetare rapporterar in personuppgiftsincidenter i relevant omfattning
3. Samtliga inrapporterade incidenter under året är färdigdokumenterade och avslutade i diariet[1]
4. Incidenterna har följts upp och föreslagna åtgärder har vidtagits

Varje organisation ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter (PUI) 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.

4. KONSEKVENSBEDÖMNINGAR (DPIA - Data Protection Impact Assessment)

I detta avsnitt ställs fyra frågor enligt nedan:
1. Verksamheten har bedömt och dokumenterat om en personuppgiftsbehandling kräver en konsekvensbedömning (DPIA)
2. Verksamheten har rutiner för att säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar, där så krävs
3. Planerade konsekvensbedömningar har genomförts[2]
4. Åtgärder i genomförda konsekvensbedömningar finns intagna i en handlingsplan, förvaltningsplan eller liknande

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska en konsekvensbedömning (DPIA – Data Protection Impact

---

[1] Om incidenten är färdigbehandlad. Ärenden som anmälts till IMY men där IMY inte ännu återkopplat ska hållas öppna tills återkoppling fås.
[2] Konsekvensbedömningar ska i regel göras innan en personuppgiftsbehandling påbörjas, ex. innan ett nytt system köps in eller ett nytt arbetssätt introduceras.

Assessment) göras. Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt att visa att dataskyddslagstiftningen följs.

5. PERSONUPPGIFTSBITRÄDEN

I detta avsnitt ställs fyra frågor enligt nedan:
1. Verksamheten har kartlagt sina samtliga externa parter/leverantörer[3] och bedömt ifall dessa är personuppgiftsbiträde/gemensamt personuppgiftsansvarig
2. Verksamheten har tecknat personuppgiftsbiträdesavtal (PUB-avtal) med sina biträden eller reglerat dessa i ett reglemente (gäller mellan nämnder)
3. Verksamheten har kontrollerat om personuppgifter överförs till tredje land (ett land utanför EU/ESS)[4]. Om uppgifter överförs till tredjeland har lagligheten kontrollerats.
4. Verksamheten har följt upp personuppgiftsbiträdesavtalen[5]

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part/leverantör som behandlar personuppgifter åt den personuppgiftsansvariga. Reglemente ska upprättas mellan nämnder i stället för personuppgiftsbiträdesavtal. Den externa parten/leverantören är då biträde och avtalet ska reglera att personuppgifter behandlas och skyddas efter instruktioner från den personuppgiftsansvarige.

Om två parter gemensamt bestämmer syftet rör det sig om ett gemensamt personuppgiftsansvar och då ska ett datadelningsavtal upprättas.

6. ARKIVERING OCH GALLRING

I detta avsnitt ställs två frågor enligt nedan:
1. Verksamhetens informationshanteringsplan/

---

[3] Dvs. kontrollerat vilka externa parter behandlar verksamhetens personuppgifter - genom lagring, åtkomst, överföring eller liknande.
[4] Tredjelandsöverföring sker när personuppgifter behandlas i ett land utanför EU/EES. Tredjelandsöverföring omfattar även underbiträden till personuppgiftsbiträden (PUB). Det betyder att verksamheten behöver kontrollera vilka underbiträden ett personuppgiftsbiträde anlitar. Tredjelandsöverföring är enbart tillåten under särskilda förutsättningar och lagligheten måste därför kontrolleras.
[5] Behöver göras regelbundet, ju känsligare personuppgifter biträdet hanterar desto viktigare är att uppföljning görs återkommande. Uppföljningen kan med fördel genomföras inom portföljstyrningen.

hanteringsanvisningar är upprättad, komplett och aktuell
2. Arkivering och gallring genomförs enligt informationshanteringsplanen/ hanteringsanvisningar

Lagringsminimering är en av dataskyddsprinciperna som anger att personuppgifter endast får behandlas så länge de behövs för ändamålet. Lagringsminimering innebär att det ska vara ordning och reda bland verksamhetens information, att information arkiveras och gallras enligt informationshanteringsplanen/hanteringsanvisningarna.

7. REGISTRERADES RÄTTIGHETER

I detta avsnitt ställs fyra frågor enligt nedan:
1. Verksamheten har rutiner för utlämnade av registerutdrag (rätten till tillgång)[6]
2. Verksamheten har informerat enskilda om hur personuppgifter hanteras (rätt till information)
3. Verksamheten har en rutin/process för att hantera övriga rättigheter, dvs. begäran om radering, rättelse, invändning och begränsning (samt dataportabilitet, om tillämplig)
4. Om automatiskt beslutsfattande används, har verksamheten kontrollerat att det är förenligt med artikel 22 GDPR

Registrerade har ett antal rättigheter avseende sina personuppgifter:

- Rätt att kontakta en personuppgiftsansvarig för att få besked om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”)
- Rätt att få information om vilka personuppgifter hanteras och hur de används (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 dessa (Rätten att göra invändningar och begära begränsning)
- Rätt att inte bli föremål för automatiskt beslutsfattande[7]
- 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)

[6] Rutinen ska säkerställa att information i samtliga lagringsytor/system som verksamheten ansvarar för söks igenom och att den information som lämnas motsvarar kraven i GDPR.
[7] Beslut som fattas utan att en fysisk person är inblandad.

Verksamheter hanterar generellt personuppgifter i stor omfattning vilket kräver att det finns utarbetade processer på plats om hur en enskild kan utöva sina rättigheter, särskilt vad gäller rätten till tillgång (registerutdrag).

8. KÄNSLIGA OCH EXTRA SKYDDSVÄRDA PERSONUPPGIFTER

I detta avsnitt ställs två frågor enligt nedan:
1. Om verksamheten hanterar känsliga personuppgifter, har det säkerställts att ett undantag enligt artikel 9 GDPR finns
2. Verksamheten har rutiner för hur och var känsliga och extra skyddsvärda personuppgifter får hanteras. Rutinerna har kommunicerats till medarbetare (på introduktion, årligen på APT eller liknande)

Det finns ett generellt förbud mot att använda känsliga personuppgifter[8] i dataskyddsförordningen. Behandling av känsliga personuppgifter är enbart tillåtet om något av undantagen är tillämpligt. Det finns personuppgifter som kallas extra skyddsvärda[9] dessa kräver inte ett undantag för att det ska vara tillåtet att behandla dem. Behandling av känsliga och extra skyddsvärda personuppgifter kräver att de skyddas med höga säkerhetsåtgärder (tekniska och organisatoriska).

9. INFORMATIONSSÄKERHET

I detta avsnitt ställs sex frågor enligt nedan:
1. Verksamheten har informationsklassat sina informationstillgångar
2. Verksamhetens system har framtagen handlingsplan i verktyget KLASSA[10]
3. Åtgärder från handlingsplanen i KLASSA finns intagen i systemets förvaltningsplan[11]
4. Verksamheten har behörighetsstyrt tillgång till verksamhetens personuppgifter enligt principen lägsta behörighet[12]
5. Verksamhetens riskanalyser inkluderar även informationssäkerhet (RSA)
6. Verksamheten har med informationsrisker i sin kontinuitetsplan

---

[8] Beskrivning av känsliga personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter
[9] Beskrivning av extra skyddsvärda personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter
[10] Leds av portföljansvarig.
[11] Leds av portföljansvarig.
[12] Dvs. att åtkomst till information enbart ges till de som behöver informationen för sitt arbete.

Integritet och konfidentialitet är en dataskyddsprincip som handlar om att säkerställa att inga personuppgifter röjs för obehöriga (konfidentialitet), är tillgängliga när de behövs (tillgänglighet) och är korrekta (riktighet). Detta säkerställs genom ett aktivt informationssäkerhetsarbete.