ÅRSRAPPORT 2021
Drn NTN 2022/115

Nämnd och personuppgiftsansvarig
Natur- och trafiknämnden

Dataskyddsombudets årsrapport 2021

Dataskyddsombud
Hanna Virtanen

Datum 2022-05-04

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 natur- och trafiknämndens efterlevnad av dataskyddsförordningen fördelat på nio områden. Områdena beskrivs närmare i rapporten nedan. Granskningen har utgått från ett antal kontrollpunkter som utgör konkreta krav i dataskyddsförordningen. Kontrollpunkterna återfinns i bilaga till årsrapporten.

Rapporten lämnas av nämndens Dataskyddsombud. Dataskyddsombud är en roll som varje nämnd är skyldig att utse enligt dataskyddsförordningen och har i uppdrag att granska och rapportera om nämndernas 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). Nacka kommuns nämnder har beslutat att ha ett gemensamt dataskyddsombud och att lokalt på varje enhet ha utsedda dataskyddssamordnare, som bistår enhetschef i hantering av GDPR-relaterade frågor och hanteringar. Denna rapport överlämnas till nämnden som en del av dataskyddsombudets uppdrag.

Nämndens efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas nämndens efterlevnad av dataskyddsförordningen inom nio områden och baserat på de kontrollpunkter som ingått i granskningen. Områdena beskrivs under respektive rubrik nedan tillsammans med en sammanfattning av nämndens efterlevnad på området.

1. Registrera personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska enligt artikel 30 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.

Nämndens registerförteckning bedöms vara komplett men informationen har delvis inte uppdateras sedan 2019 och behöver därmed ses över.

2. Grundläggande principer

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar övriga krav på dataskydd. Principer handlar bland annat om att ha en rättslig grund, enbart behandla så många personuppgifter som behövs för ett visst syfte, iaktta proportionalitet, inte spara längre än de behövs och ha tillräcklig säkerhet.

Nämnden gör en kontroll av om grundläggande principerna följs i samband med att registerförteckningen upprättas och uppdateras. Samtycke används inte som rättslig grund.

3. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter 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.

I Nacka kommun finns en central process för personuppgiftsincidenter som följs av nämnden. Inga incidenter har rapporterats under 2021.

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.

Personuppgiftsbehandlingar som kräver konsekvensbedömningar har identifierats men konsekvensbedömningarna har ännu inte utförts.

[1] Registrerade = enskilda vars personuppgifter hanteras

5. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal 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 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.

Nämndens biträden utgörs i huvudsak av leverantörer av nämndens system och personuppgiftsbiträdesavtal finns tecknade med dessa. PUB-avtalen har dock ännu inte följts upp.

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, att information rensas, arkiveras och gallras. Informationshanteringsplanen (IHP) är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras.

Nämnden har en aktuell informationshanteringsplan men arkivering/gallring har inte i alla delar utförts enligt planen.

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)*

Kommuner 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).

I Nacka kommun finns en central process för utlämnande av registerutdrag (rätten till tillgång) som följs av nämnden. Rätten till information uppfylls inte helt då information inte lämnas i enlighet med dataskyddsförordningens krav. Vad gäller övriga rättigheter finns ingen särskild process/rutin men samtidigt får nämnden få förfrågningar kring dessa rättigheter.

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

8. Känsliga och extra skyddsvärda personuppgifter

Det finns ett generellt förbud mot att använda 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.

Känsliga personuppgifter i form av hälsa behandlas inom vissa ärendeprocesser, även extra skyddsvärda personuppgifter förekommer. Rutiner finns men de behöver ses över för att säkerställa att dessa typer av uppgifter skyddas i alla delar av handläggningen.

9. Informationssäkerhet

En viktig dataskyddsprincip 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.

Vissa informationssäkerhetsanalyser, exempelvis informationsklassning och handlingsplaner i SKR:s KLASSA-verktyg har gjorts, men analyserna behöver genomföras systematiskt och följas upp.

Sammanfattning av nämndens efterlevnad och dataskyddsombudets rekommendationer

Inom alla områden har nämnden genomfört ett arbete för att anpassa sig till dataskyddsförordningen krav, men ett visst arbete kvarstår fortfarande för att efterleva förordningen i helhet. Följande rekommendationer ges till nämnden för att kunna uppfylla kraven inom samtliga områden:

- Utföra planerade konsekvensbedömningar (DPIA).
- Ta fram rutin/process för uppföljning av personuppgiftsbiträdesavtalen (kan med fördel göras inom objekts-/systemförvaltningen).
- Säkerställa att arkivering och gallring utförs i enlighet med nämndens informationshanteringsplan.

---

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

- Ge enskilda komplett och tydlig information om hanteringen av sina personuppgifter enligt dataskyddsförordningen krav.
- Se över rutiner för känsliga och/eller extra skyddsvärda uppgifter för att säkerställa att dessa typer av uppgifter genomgående hanteras säkert.
- Fortsätta med ett systematiskt informationssäkerhetsarbete genom att följa upp informationsklassningar och genomföra övriga analyser som syftar till att nämndens information omfattas av den säkerhet informationen kräver.