ÅRSRAPPORT 2021
Dnr KFKS 2022/364

Nämnd och personuppgiftsansvarig
Kommunstyrelsen

Dataskyddsombudets årsrapport 2021

Dataskyddsombud
Hanna Virtanen

Datum 2022-04-20

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 kommunstyrelsens efterlevnad av dataskyddsförordningen fördelat på nio områden. Områdena beskrivs närmare i rapporten nedan. Årets granskning omfattar följande verksamheter/enheter: välfärd samhällsservice, välfärd skola (verksamhetsstöd), personalenheten, kommunikationsenheten och enheten för fastighetsförvaltning. 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 dataskyddsförordningens 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.

Några personuppgiftsbehandlingar finns registrerade i nämndens registerförteckning men är i många delar ofullständig.

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.

En kontroll av om de grundläggande principerna följs görs i samband med att registerförteckningen upprättas och uppdateras. Samtycke används som rättslig grund främst för publicering av bilder och filmer och delning av information. Vägledning finns för när samtycke kan användas som rättslig grund men en kontroll av enskilda situationer har inte gjorts i granskningen.

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. Incidenterna har dokumenterats, följts upp och ärendena avslutats med några få undantag. Under 2021 har 28 incidenter rapporteras inom nämnden, varav 6 anmäldes vidare till IMY. IMY har avslutat samtliga ärenden utan åtgärd. Den vanligaste incidenten handlar om att känslig information hamnat eller riskerat att hamna hos obehöriga.

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.

[1] Registrerade = enskilda vars personuppgifter hanteras

Kontroll har gjorts om en konsekvensbedömning (DPIA) krävs och har också i flera fall genomförts, men inte inom samtliga verksamhetsområden.

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. I de flesta fall har personuppgiftsbiträdesavtal tecknats men inte med samtliga biträden. Nämnden har biträden där överföring av personuppgifter sker till USA men huruvida detta är förenligt med dataskyddsförordningens krav har inte kontrollerats i alla situationer. Uppföljning av PUB-avtalen har skett, men inte på ett systematiskt sätt.

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.

Inom de flesta verksamheter finns en beslutad informationshanteringsplan, men för några saknas fortfarande en IHP. Inom vissa verksamhetsområden saknas även rutiner för gallring och arkivering.

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).

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

I Nacka kommun finns en central process för utlämnande av registerutdrag (rätten till tillgång) som följs av nämnden. I processen är det dock otydligt hur personuppgifter i centrala system ska hanteras, varför utdraget till den enskilde riskerar att vara ofullständig. Enskildas rätt till information uppfylls delvis då information visserligen lämnas av de flesta verksamheter på något sätt men kraven i dataskyddsförordningen är inte helt uppfyllda. För övriga rättigheter finns inte några fastställda rutiner för alla verksamheter, men i granskningen framkommer att enskilda inte frekvent utövar dessa rättigheter. Automatiskt beslutsfattande sker inte i dagsläget.

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.

Inom flera verksamhetsområden behandlas känsliga personuppgifter, men då registerförtekningen inte är helt komplett har inte lagligheten kontrollerats i samtliga fall. Känsliga personuppgifter ska hanteras i verksamhetssystem och rutiner saknas delvis.

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.

Informationsklassningar och bedömningar i SKR:s KLASSA-verktyg har gjorts för flera av nämndens system, men inte för samtliga. Behörighetsstyrning finns, med några få undantag.

Sammanfattning av nämndens efterlevnad och dataskyddsombudets rekommendationer

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

---

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

- Färdigställa nämndens registerförteckning genom att registrera samtliga personuppgiftsbehandlingar.
- Genomföra konsekvensbedömningar (DPIA) när dataskyddsförordningen kräver det.
- Säkerställa att personuppgiftsbiträdesavtal tecknats med samtliga biträden och införa systematisk uppföljning av avtalen. Kan med fördel göras inom system-/objektsförvaltningen.
- Ta fram informationshanteringsplaner (där så saknas) och rutiner för arkivering och gallring
- Revidera processen för registerutdrag (rätten till tillgång) för att säkerställa att ett fullständigt registerutdrag lämnas i enlighet med dataskyddsförordningens krav.
- Ge enskilda komplett och tydlig information om hanteringen av sina personuppgifter enligt dataskyddsförordningen krav. Informationen kan med fördel delvis samordnas centralt i kommunen.
- Säkerställa att rutiner finns för hantering av känsliga personuppgifter.
- 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, särskilt vad gäller känsliga personuppgifter och uppgifter som omfattas av sekretess.