NACKA KOMMUN

DSO:s årsrapport 2022
Dnr KFKS-2023-00476

Personuppgiftsansvarig
Kommunstyrelsen övriga enheter (exklusive VSS och VS)

Dataskyddsombudets årsrapport 2022

Dataskyddsombud
Hanna Virtanen

Datum 2023-05-11

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, exklusive välfärd samhällsservice och välfärd skola som presenteras i separata rapporter. Granskningen är indelad i nio områden som beskrivs närmare i rapporten nedan tillsammans de 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 överlämnas till kommunstyrelsen av nämndens dataskyddsombud inom ramen för dennes uppdrag. Dataskyddsombud är en roll som en nämnd är skyldig att utse enligt dataskyddsförordningen och har i uppdrag att granska och rapportera om den personuppgiftsansvariges 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).

Kommunstyrelsens 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

[1] Registrerade = enskilda vars personuppgifter hanteras

förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens då den anger vilka personuppgifter som behandlas, hur och varför.

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

Nämndens efterlevnad

– Delar av nämndens enheter har registrerat sina personuppgiftsbehandlingar i enlighet med kraven i GDPR. För några andra enheter saknas, delvis eller helt, en kartläggning och förteckning över personuppgiftsbehandlingarna.

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

– De enheter som förtecknat och kartlagt sina personuppgiftsbehandlingar bedöms beakta de grundläggande principerna. I övrigt är har det inte varit möjligt i denna granskning att bedöma om principerna följs. Nästan alla enheter har genomfört någon typ av GDRP utbildning för sina medarbetare under året, antingen på gemensamma möten eller i samband med introduktion för nyanställda. Sedan november 2022 finns en e-learning utbildning i GDPR som är tillgänglig för samtliga enheter och verksamheter i kommunen.

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. Under 2022 har 14 incidenter rapporterats in, varav en anmäldes vidare till tillsynsmyndigheten (IMY). De verksamheter som genomfört GDPR-utbildning har också fått information om incidenthanteringsprocessen.

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

En övergripande riskbedömning över vilka personuppgiftsbehandlingar som kräver en konsekvensbedömning är gjord, dock är inte alla konsekvensbedömningar genomförda. Dataskyddsombudet rekommenderar också att konsekvensbedömningen för sociala medier kompletteras med andra risker utöver tredjelandsöverföring och att konsekvensbedömningen för Office 365 färdigställs för att få en överblick över risker och åtgärder som krävs för att mitigera dessa.

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

Personuppgiftsbiträdesavtal (PUB-avtal) har tecknats i samband med nya upphandlingar och för äldre system i samband med att GDPR trädde i kraft. Några få PUB-avtal saknas i dagsläget, men ett arbete pågår med att säkerställa att korrekta avtal finns på plats.

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

Antagna informationshanteringsplaner finns för verksamhetsområdena, men dessa speglar inte alltid den information som hanteras inom verksamheterna och behöver därmed revideras. Arkivering och gallring utförs inte heller alltid 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

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

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.

Nämndens efterlevnad

Varje nämnd följer den kommungemensamma processen för begäran av registerutdrag (rätten till tillgång). Enheter under kommunstyrelsen är ansvariga för att samordna inkomna begäran genom att samla in uppgifter från berörda nämnder och skicka ut svaret till den registrerade. Under 2022 har registerutdrag enbart vid några tillfällen hanterats i tid. Enligt GDPR ska den registrerade få svar på sin begäran inom 30 dagar vilket inte skett. Förändringar i den kommungemensamma processen har nyligen gjorts för att säkerställa att registerutdrag skickas inom de lagstadgade tidsramarna.

Den kommungemensamma processen följer dock fortfarande inte kraven i GDPR i sin helhet då inga kopior av själva personuppgifterna (eller annan tillgång till personuppgifterna) lämnas vid en första begäran utan den registrerade måste återkomma igen för att få ta del av dem. Riktlinjer från europeiska dataskyddsstyrelsen[3] (som består av alla EU-länders tillsynsmyndigheter och ska verka för en enhetlig tillämpning av GDPR) tydliggör att rätten till tillgång innebär faktisk tillgång till de faktiska personuppgifterna som behandlas, inte enbart en beskrivning av typer av uppgifter och inom vilken process. Därutöver är nuvarande rutin för sökningar i centrala system utformad på ett sätt som kan leda till svaret till den registrerade blir felaktigt då all information inte söks igenom.

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. Informationen ska dessutom vara begriplig, dvs. kan behöva anpassas mottagaren, och vara lättillgänglig. På nacka.se har kommunen en generell sida som informerar om hur kommunen hanterar personuppgifter[4], men informationen är för generell för att en medborgare (eller annan person vars personuppgifter kommunen hanterar) ska kunna förstå hur personuppgifterna kommer hanteras och sidan innehåller inte heller all obligatorisk information.

8. Känsliga och extra skyddsvärda personuppgifter

Det finns ett generellt förbud mot att hantera känsliga personuppgifter[5] i dataskyddsförordningen. Det är enbart tillåtet om en av undantagen är tillämpliga, därför är

---

3 Guidelines 01/2022 on data subject rights - Right of access, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf .

4 https://www.nacka.se/om-webbplatsen/behandling-av-personuppgifter

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

det viktigt att veta om eventuella känsliga personuppgifter som behandlas är laglig. Förutom känsliga personuppgifter, finns det en grupp personuppgifter kallat extra skyddsvärda[6] 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.

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 informationsklassning och riskanalyser genomförts.

Nämndens efterlevnad

Informationsklassningar och riskanalyser har främst 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. Därutöver kommer ny informationssäkerhetsstrategi antas av kommunfullmäktiga som kommer att möjliggöra för ett mer systematiskt informationssäkerhetsarbete.

Sammanfattning av nämndens efterlevnad och dataskyddsombudets rekommendationer

Efterlevnaden av dataskyddsförordningen skiljer sig mellan enheterna under nämnden och därför blir den sammantagna bedömningen också att kraven i GDPR följs i många delar, men inom några områden krävs åtgärder för att uppfylla kraven i sin helhet. Respektive enhet har av dataskyddsombudet fått enhetsspecifika rekommendationer om vilka åtgärder de behöver vidta för att efterleva kraven.

---

[6] 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

Nedan sammanfattas de åtgärder som krävs för att kommunstyrelsens enheter (exklusive VS och VSS) ska anses följa kraven i GDPR (utifrån de delar som ingått i årets granskning):

- Kartläggning och förteckning över samtliga personuppgiftsbehandlingar i nämndens registerförteckning.
- Uppföljning av hur många medarbete gått utbildning i GDPR för att säkerställa att respektive medarbetare har kunskap om dataskydd och personuppgiftshantering.
- Färdigställande av de konsekvensbedömningar som ännu inte gjorts och komplettering av befintliga konsekvensbedömningen enligt rekommendationen ovan i punkt 4.
- Framtagande av personuppgiftsbiträdesavtal (PUB-avtal), där så saknas.
- Revidering informationshanteringsplaner, där så krävs och att gallring och arkivering kan genomföras i samtliga system och lagringsytor där nämndens information hanteras.
- Uppföljning av svarstider för registerutdrag och en översyn av processen för att säkerställa att den är lagenlig (se även paragrafen nedan).
- Framtagande av komplett, tydlig och lättillgänglig information om hanteringen av sina personuppgifter enligt dataskyddsförordningen krav (se även paragrafen nedan).

Kommunstyrelsen har enligt nämndens reglemente ansvar för kommunens säkerhetsarbete och i det ansvaret ligger även samordning av dataskyddet. Utifrån granskningen av kommunstyrelsen och vad som framkommit i övriga nämnders granskningar ges följande rekommendation till kommunstyrelsen i rollen som ansvarig för samordning av kommunens dataskyddsarbete:

- Översyn av processen för registerutdrag (rätten till tillgång) för att säkerställa att den hanteras lagenligt (se punkt 7 ovan).
- Samordna kommunens insatser vad gäller kravet om rätten till information genom bland annat uppdatering av den kommungemensamma informationssidan[7]. I nästan alla nämnders granskningar finns brister i hur information ges till registrerade. Informationen måste anpassas till varje situation och registrerad, därmed måste varje enhet/verksamhet själv identifiera sina registrerade och säkerställa att informationen ges korrekt. I vissa delar dock finns en fördel av att samordna informationen, genom att enheter/verksamheter i vissa delar kan hänvisa till en kommungemensam text (och vice versa) och eller genom att vissa enheter har ansvar för en viss kategori registrerade, exempelvis att personalenheten ansvarar för information till kommunen anställda, även om det är någon annan enhet som tar initiativ till och ansvarar för personuppgiftsbehandlingen.

[7] https://www.nacka.se/om-webbplatsen/behandling-av-personuppgifter/