NACKA KOMMUN

ÅRSRAPPORT 2020
Diarienummer

**Nämnd och personuppgiftsansvarig**
*Kommunstyrelsen*

# Dataskyddsombudets årsrapport 2020

**Dataskyddsombud**
Mattias Widegren

**Datum** 2021-05-01

## Innehåll

# Inledning

Dataskyddsförordningen (GDPR) är den lagstiftning som reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Personuppgift är varje 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 ansvarig för att förordningens krav följs.

Kommunen valde 2018 en införandemodell för GDPR med tolv (12) fokusområden, som än idag utgör utvärderingsmodell för varje nämnds införandegrad och effektivitet avseende efterlevnaden av kravbilden i GDPR.

Fokusområden GDPR:

- Registrerade personuppgiftsbehandlingar
- Rapportera personuppgiftsincidenter
- Konsekvensbedömningar (DPIA)
- Personuppgiftsbiträdesavtal (PUB-avtal)
- Lagringsminimering, arkivering och gallring av personuppgifter
- Registerutdrag (rätten till tillgång)
- E-post
- Systemsäkerhet
- Behörighet
- Samtyckeshantering
- Informationsplikt
- Efterlevnad

Denna rapport utgår från de tolv fokusområdenas status och från de rekommendationer som Dataskyddsombudet generellt anser att kommunens nämnder behöver förbättra. I likhet med den revisionsrapport för GDPR som Ernst & Young genomförde för kommunrevisorernas räkning anser Dataskyddsombudet att ”fotarbetet” i kommunens enheter fungerar bra, men att det saknas tydliga avrapporteringsvägar till ledningsfunktioner och att styrdokument inte på ett effektivt sätt når medarbetarna. Därtill anser Dataskyddsombudet att det generellt behövs en systematisk egenkontroll för varje enhet för att underlätta både rapportering till ledning och för att medvetandegöra enhetsledning om eventuella förbättringsbehov.

Rapporten lämnas av nämndens Dataskyddsombud. Dataskyddsombud är en roll som varje nämnd är skyldig att utse enligt förordningen och har i uppdrag att granska och rapportera om nämndernas efterlevnad av förordningen. 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 lämnas till nämnden som en del av dataskyddsombudets uppdrag.

## Sammanfattning av 2020 års arbete med dataskydd

Nämnden har under 2020 fortsatt arbetet enligt den plan som lades fast under 2018 inför införandet av Dataskyddsförordningen. Planen omfattar de tolv (12) fokusområden som nämndes i inledningen och under 2020 har generellt arbetet inriktats på hantering av begäranden av registerutdrag, personuppgiftsincidenthantering, personuppgiftsbiträdesavtal och genomförande av konsekvensbedömningar.

# Nämndens efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas nämndens efterlevnad av dataskyddsförordningens krav utifrån de 12 prioriterade fokusområden som tidigare beslutats av stadsledningskontoret. De 12 områdena beskrivs under respektive punkt nedan tillsammans med en sammanfattning av nämndens efterlevnad på området.

## 1. Registrera personuppgiftsbehandlingar

En grundläggande förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens regler är att veta vilka personuppgifter som behandlas och varför (i vilket syfte). Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade, typer av personuppgifter och lagringstid framgår. På kommunens hemsida presenteras varje nämnds personuppgiftsbehandlingar, och detta register utgör den publika registerförteckningen. Därtill finns en databas där samtliga arbetsdokument och detaljerad information för varje behandling redovisas. Enheternas dataskyddssamordnare registrerar och uppdaterar informationen i databasen med stöd av dataskyddsombudet.

Kommunstyrelsen har 28 personuppgiftsbehandlingar registrerade och presenterade på kommunens hemsida. Registerförteckningen bedöms vara komplett och innehåller i stort sett all nödvändig information, endast någon enstaka information fattas.
I databasen finns däremot 299 registreringar för nämnden, vilket inte korrelerar till den publika presentationen. Databasen måste kontinuerligt underhållas och aktualitetskontrolleras, och varje registrering skall kopplas till en behandling i den publika registerförteckningen.
Eftersom det finns en stor diskrepans mellan databasens registreringar och det publika registret, rekommenderas kommunstyrelsen att genomföra en genomgång och städning av databasen.
Det finns ett stort antal registreringar i databasen som inte uppdaterats sedan 2019 och tidigare, och nämnden uppmanas att säkerställa att de årligen uppdateras och aktualitetskontrolleras.

## 2. Rapportera personuppgiftsincidenter

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

I Nacka kommun finns en central process för personuppgiftsincidenter som följs av nämnden. Kommunstyrelsen rapporterade under 2020 31 incidenter, varav 5 anmäldes till Integritetsskyddsmyndigheten. Samtliga av de anmälda incidenterna har avslutats av Integritetsskyddsmyndigheten utan åtgärd. Rapporterade incidenter följer även rutiner för

nämndens avvikelsehantering för att förhindra framtida incidenter. Av stor vikt är organisationens lärande från inträffade incidenter, och nämnden uppmanas analysera och säkerställa att varje enhet redovisar lärdomar och aktiviteter utgående från dessa. Av de 31 incidenterna som hanterades under 2020 är fortfarande 13 stycken ej avslutade i diariet, och därtill finns 7 fortfarande oavslutade ärenden sedan 2018-2019. Kommunstyrelsen uppmanas att säkerställa att dokumentationen slutförs och alla ärenden avslutas.

## 3. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning.
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.

Något centralt register över vilka konsekvensregistreringar som genomförts inom nämndens ansvarsområde finns inte, varför nämnden uppmanas dokumentera förekomst och den eventuella bristen.

## 4. 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.
Något centralt register över vilka leverantörer som har personuppgiftsbiträdesförhållande till nämnden finns inte, varför nämnden rekommenderas att uppdra åt dataskyddssamordnarna att dokumentera status och identifiera eventuella brister.

## 5. 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 är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras. Någon centraliserad strukturerad lagring av informationshanteringsplanen finns inte, varför Dataskyddsombudet inte kunnat granska den. Nämnden uppmanas att

säkerställa att enheternas dataskyddssamordnare uppdras att dokumentera informationshanteringsplanerna i samma databas där personuppgiftsbehandlingarna dokumenteras. hanteras.

## 6. Registerutdrag (rätten till tillgång)

Registerutdrag eller rätten till tillgång är en rättighet i dataskyddsförordningen som varje enskild har i förhållande till sina personuppgifter. Rättigheten innebär att varje person har rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa. Kommuner hanterar generellt personuppgifter i stor omfattning vilket kräver att det finns utarbetade processer på plats om hur ett registerutdrag ska hanteras.

I Nacka kommun finns en central process för registerutdrag som följs av nämnden. Denna process följer dataskyddsförordningens krav och under 2020 har 5 registerutdrag hanterats av nämnden. Processen för att producera registerutdrag är komplex och nämnden rekommenderas att se över dess effektivitet avseende ledtider och innehållets kvalitet.

## 7. E-post

I dataskyddsförordningen finns inte som tidigare i personuppgiftslagen ett undantag för personuppgifter i ostrukturerat material, vilket betyder att även personuppgifter i ett e-postmeddelande omfattas av dataskyddslagstiftning. Detta ställer höga krav på att även hanteringen av e-post följer dataskyddsprinciperna, exempelvis att personuppgifter endast behandlas för specifika syften och inte sparas längre än nödvändigt samt att känsliga personuppgifter skyddas med säkerhetsåtgärder.

I Nacka kommun finns en framtagen guide för säker e-posthantering som beskriver hur e-post hanteras på ett säkert och med dataskyddsförordningen förenligt sätt. Rutinen tas upp kontinuerligt med medarbetare och rutiner för att hantera känsliga och extra skyddsvärda personuppgifter på ett säkert sätt har implementerats.
Under 2020 har ett system för överförande av känslig information införts, Säkra Meddelanden. Därtill har funktioner i e-postsystemet införts där avsändaren uppmärksammas om personuppgiftsinformation ingår i meddelandet. Dessa båda åtgärder har inneburit avsevärda framsteg med att reducera riskerna för behövliga överföringar av personuppgifter.

## 8. Systemsäkerhet

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). En metod för att ta fram krav på ett system som uppfyller dessa aspekter är

informationsklassning som visar hur skyddsvärd informationen är utifrån de tre aspekterna. System kan därefter anpassas så att kraven motsvarar informationens skyddsvärde. Informationsklassningen görs i systemet KLASSA, levererat och utvecklat av SKR.

Kommunstyrelsen har 13 system registrerade för informationsklassificering, varav tre helt saknar handlingsplan och fyra inte har uppdaterats sedan mitten av 2018. För de system som saknar uppdateringar (eller helt handlingsplan) rekommenderas kommunstyrelsen att genomföra en aktualitetskontroll och säkerställa att informationsklassificeringen uppdateras som ett led i systemförvaltningen.

## 9. Behörighet

Korrekt hantering av behörigheter till system och andra ytor som lagrar personuppgifter är en förutsättning för att inte personuppgifter ska bli tillgängliga för obehöriga (dvs. att personuppgifternas konfidentialitet skyddas) och för att personuppgifter inte behandlas för olovliga syften. Korrekt hantering av behörigheter betyder att behörighet till personuppgifter ges utifrån användarens behov av att behandla uppgifterna och att dessa behörigheter regelbundet ses över.

Nämnden har framtagna rutiner för behörigheter till sin information, både för anställda inom nämnden och anordnare externt som har tillgång till informationen. Däremot finns behov av att rutinerna även säkerställer att anställda som inom kommunen byter tjänst också får ändrade behörigheter utifrån sina nya arbetsuppgifter. Nämnden rekommenderas att använda kontrollplanen för att säkerställa att behörigheter kontinuerligt ses över.

## 10. Samtycke

I dataskyddsförordningen skärptes kraven på hur och när samtycke kan användas som stöd för en personuppgiftsbehandling. För offentlig verksamhet betyder det att det numera finns begränsade möjligheter att använda samtycke eftersom ett samtycke måste kunna ges helt frivilligt och en myndighet ofta står i maktpositionen gentemot en enskild.

Det har inte framkommit i granskningen att nämnden använder samtycke som rättslig grund för att behandla personuppgifter. Nämnden rekommenderas att använda kontrollplanen för att dokumentera detta.

## 11. Informationsplikt

Informationsplikten i dataskyddsförordningen betyder att inga personuppgifter får behandlas utan att en enskild vet om detta, detta krav gäller oavsett om uppgifterna samlas direkt in av en enskild eller från en annan källa. Det finns i förordningen dessutom krav på

vilken typ av informationen som ska ges samt att detta ska ske på ett enkelt och lättillgängligt sätt.
Ett sammanställt och dokumenterat sätt att överblicka de informationstexter som skall föregå varje personuppgiftsbehandling finns inte, varför nämnden rekommenderas att uppdra dataskyddssamordnarna att årligen säkerställa informationens aktualitet och korrekthet.

## 12. Efterlevnad

Efterlevnad handlar om att nämnden ska kunna visa att dataskyddsförordningens krav följs.

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

- Genomföra konsekvensbedömningar där dataskyddsförordningen kräver det. Dokumentationen skall sparas i registerförteckningens databas.
- Säkerställa att personuppgiftsbiträdesavtalen uppfyller dataskyddsförordningens krav, särskilt vad gäller information om underbiträden. Detta arbete kan göras i samband med en avtalsuppföljning för att kontrollera att ett biträde även lever upp till kraven på personuppgiftshantering.
- 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.
- Ge enskilda komplett och tydlig information om hanteringen av sina personuppgifter enligt dataskyddsförordningen krav.