

## **Nacka kommun**

Granskning av efterlevnad  
Dataskyddsförordningen GDPR

Juni 2020

## Sammanfattning

EY har på uppdrag av Nacka kommuns förtroendevalda revisorer genomfört en granskning av kommunens hantering av personuppgifter och efterlevnad av dataskyddsförordningen (The General Data Protection Regulation, GDPR).

Granskningens syfte har varit att ge en övergripande förståelse av huruvida kommunen som helhet bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur väl man uppfyller de åtgärder som förordningen stipulerar. Analysen har baserats på intervjuer med identifierade nyckelpersoner i verksamhetens personuppgiftssäkerhetsarbete samt genomgång av insamlad styrdokumentation. Analys och iakttagelser har faktagranskats av de identifierade nyckelpersonerna.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under maj till juni 2020. Enligt metoden bedöms verksamhetens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Den genomsnittliga mognadsgraden är baserad på snittet av mognadsgraden för de respektive 12 områdena.

Baserat på den analys och granskning som genomförts bedöms Nacka kommun ha den genomsnittliga mognadsgraden 3,4 av 5,0. Det är en högre mognadsgrad än vad EY har observerat att genomsnittet är för en kommun. Nacka har arbetat ambitiöst med personuppgiftsfrågor och nyckelpersonerna i den centrala dataskyddsorganisationen har kommit långt i sitt arbete.

Överlag bedöms mognadsgraden vara högst inom organisation och ansvar, riskhantering samt utbildning. Nacka har ett dataskyddsombud (DSO) på heltid, en väl utvecklad organisation kring dataskyddsfrågor och har ägnat mycket resurser åt utformning av rutiner samt implementation och medvetenhet bland anställda. Mognadsgraderna i styrning och kontroll bedöms däremot vara något lägre då dessa områden i viss mån har prioriterats lägre när man har fokuserat på implementation av praktisk hantering av dataskyddsfrågor. En ej optimerad kontroll påverkar även flera andra områden negativt i bedömningen då en högre mognadsgrad generellt sett är beroende av systematisk uppföljning inom varje område.

Den viktigaste förbättringspunkten är att upprätta mer formaliserade rutiner för granskning av efterlevnad. Syftet är att minska risker för otillbörlig behandling av personuppgifter på grund av att man missat efterlevnad av rutiner. EY rekommenderar därför kommunen att förbättra sin internkontroll genom att skapa ett rapporteringskrav med fastställd frekvens och innehåll som de kommunala verksamheterna kan utgå från, för att säkerställa att uppföljning och förbättringsarbete sker effektivt i samtliga enheter.

## Innehållsförteckning

|   |           |
|---|-----------|
| <b>Sammanfattning .....</b>                                       | <b>1</b>  |
| <b>1. Inledning .....</b>   | <b>3</b>  |
| 1.1. Bakgrund .....   | 3         |
| 1.2. Syfte .....  | 3         |
| 1.3. Avgränsning .....  | 4         |
| 1.4. Metod .....  | 4         |
| 1.5. Definitioner .....   | 5         |
| <b>2. Analys .....</b>  | <b>6</b>  |
| 2.1. Nuläge och iakttagelser .....                                | 8         |
| 2.2. Övergripande rekommendationer .....                          | 15        |
| <b>3. Slutsatser .....</b>  | <b>16</b> |
| <b>4. Bilaga 1: Förteckning över intervjuade funktioner .....</b> | <b>17</b> |
| <b>5. Bilaga 2: Dokumentförteckning .....</b>                     | <b>18</b> |
| <b>6. Bilaga 3: Definitioner .....</b>                            | <b>19</b> |

# 1. Inledning

## 1.1. Bakgrund

Den nya dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679 gäller i hela EU och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998. Det främsta syftet med dataskyddsförordningen är skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället.

I jämförelse med PUL ställer Dataskyddsförordningen högre krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter. Vid överträdelse av förordningens artiklar föreligger skärpta sanktioner:

- ▶ Både offentliga och privata institutioner skall kunna beläggas med sanktioner utefter samma bedömningskriterier (upp till 10 MSEK för offentliga verksamheter beroende på överträdelsens allvarlighetsgrad).
- ▶ Obligatorisk överträdelseanmälan rörande personuppgiftsincidenter skall göras till den lokala tillsynsmyndigheten inom 72 timmar efter att incidenter har uppdragats.
- ▶ Individer har rätt till ersättning i form av skadestånd till följd av överträdelser av förordningen av en personuppgiftsansvarig eller ett personuppgiftsbiträde.

Datainspektionen är den tillsynsmyndighet som ansvarar för uppföljning och kontroll av att lag och förordning efterlevs. I oktober 2018 publicerade Datainspektionen en "sammanställning av resultatet från granskning av dataskyddsbud". Granskningen omfattade såväl offentlig som privat sektor. Det konstateras att det är en marginell skillnad i efterlevnaden av reglerna mellan myndigheter och privata aktörer. Inga primärkommuner ingick i granskningen. Av totalt 66 tillsynsärenden beslutade inspektionen att ge reprimander i 57 fall. I två fall fick tillsynsobjekten ett föreläggande och sju fall avslutades utan åtgärd. Datainspektionen har också inlett andra inspektioner inom ramen för dataskyddsförordningens efterlevnad.

Då Nacka kommun med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna beslutat att genomföra en granskning av efterlevnaden av dataskyddsförordningen för kommunen som helhet.

## 1.2. Syfte

Syftet med granskningen är att ge en övergripande förståelse av huruvida Nacka kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur man uppfyller de åtgärder som förordningen stipulerar.

### 1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policys. Granskningen är begränsad till arbetet som Nacka kommun bedriver på central nivå. Intervjuer har endast utförts med representanter central nivå och inte med representanter i förvaltningarna. Inga bolag har granskats. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

### 1.4. Metod

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner samt genomgång av relevant styrdokumentation (se Bilaga 2: *Dokumentförteckning*). Granskningen är utförd i enlighet med god praxis och med utgångspunkt i EY:s metod för granskning av mognadsgrad gentemot dataskyddsförordningen.

Metoden består av ett ramverk med 116 frågor. Dessa frågor är kategoriserade över 12 områden kopplade till dataskyddsförordningen och täcker in de områden som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i personuppgiftshanteringen. Besvarandet av frågorna som innefattas av ramverket sker genom arbetsmöten med GDPR-specialister från EY. Våra specialister sammanställer svaren och redogör för avvikelser inom ovan nämnda 12 områden. En bedömning av mognadsgrad sker på en femgradig skala utifrån observationerna.

Frågorna är både direkt kopplade till krav från förordningen och indirekt kopplade genom att täcka exempelvis styrning och underhåll av arbetet med att upprätthålla regeluppfyllnaden. För enkelhetens skull används ordet "krav" synonymt i rapporten oavsett om det avser en direkt eller indirekt koppling. Metoden understryker premissen att det är viktigt att inte enbart granska huruvida enskilda kontroller är på plats och enskilda krav är täckta; det är även av stor vikt att säkerställa att styrning och uppföljning av regeluppfyllnad sker systematiskt.

#### De 12 områdena som granskats inom uppdraget är:

1. Styrande dokument/styrning
2. Riskhantering
3. Kontroll
4. Organisation och ansvar
5. Behandling av personuppgifter
6. Val av skyddsåtgärder
7. Inbyggt dataskydd
8. Hantering av leverantörsrelationer
9. Hantering av incidenter
10. Information till registrerade
11. Begäran från registrerade
12. Profilerings

### Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. **Begynnande** – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. **Upprepbar** – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. **Definierad** – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. **Förvaltad** – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. **Optimerad** – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan ett område med grön färgkod exempelvis ändå sakna viktiga kontroller. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext nedan i granskningsrapporten.

Inledningsvis har underlag såsom policyer, strategi- och styrdokument och dylikt samlats in för analys. Därefter höll EYs GDPR-specialister ett arbetsmöte med nyckelpersoner inom respektive granskad verksamhets informationssäkerhetsarbete (se Bilaga 1: *Förteckning över intervjuade funktioner*). Under arbetsmötena avhandlades samtliga 12 områden. Efter att EY analyserat resultatet av arbetsmötena sammanställdes ett rapportutkast som faktagranskades av de intervjuade. EY genomförde sedan justeringar och uppdateringar av rapporten som även kvalitetssäkrades av EY:s verksamhetsrevisorer, varefter de förtroendevalde revisorerna på kommunen erhöll en slutlig rapport med övergripande rekommendationer för fortsatt arbete.

### Tidsplanen för arbetet såg ut enligt följande:

- April 2020 – Förberedelser, planering och insamling av dokumentation.
- Maj 2020 – Dokumentanalys, utförande av arbetsmöte (2020-05-14), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport, samt faktagranskning av intervjuade nyckelpersoner.
- Juni 2020 – Kvalitetssäkring av EY:s verksamhetsrevisorer och slutgiltig presentation för kommunens förtroendevalda revisorer.

## 1.5. Definitioner

Se bilaga 3.

## 2. Analys

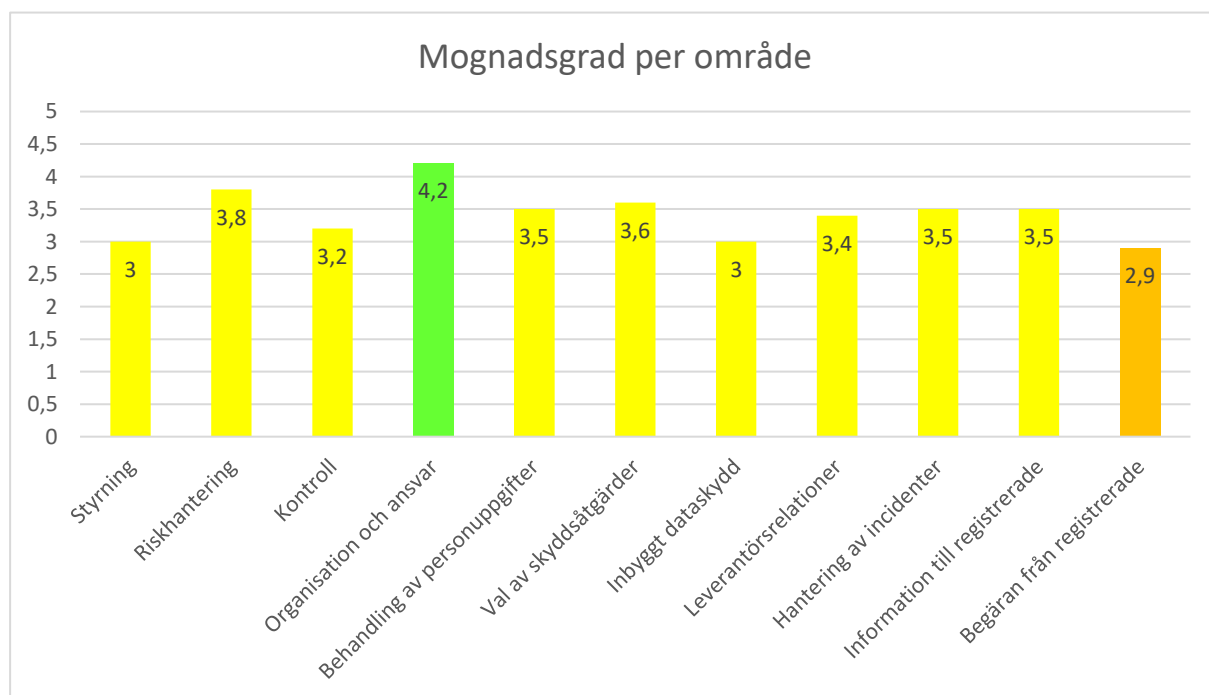
Baserat på utförd granskning konstateras att Nacka kommun på central nivå har en förhållandevis god mognadsgrad inom personuppgiftshantering jämfört med vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.

Ansvariga personer arbetar ambitiöst med dataskydd och det är tydligt att Nacka har dedikerat mycket resurser för detta arbete. Från centralt håll har de ansvariga prioriterat praktiska guider och implementationer av arbetet med personuppgiftssäkerhet, vilket avspeglar sig i väl dokumenterade rutiner och omfattande utbildningsinsatser för verksamhetens medarbetare.

Det finns ett antal identifierade förbättringsområden. Trots att kommunen har en central dataskyddsorganisation med goda resurser, har styrdokumentet inte hunnit uppdateras enligt kraven i dataskyddsförordningen. Styrningen är inte heller komplett med avseende på kontrollområdet, där det inte finns fastslagna granskningsplaner. En brist på väletablerade kontrollrutiner från centralt håll medför risker då mycket ansvar ligger på nämnderna som är personuppgiftsansvariga och ansvarar för behandlingen av personuppgifter i deras verksamheter. De större nämnderna har generellt sett inte kommit lika långt i sitt arbete som de mindre nämnderna, vilket är noterbart då riskerna där kan antas vara högre.

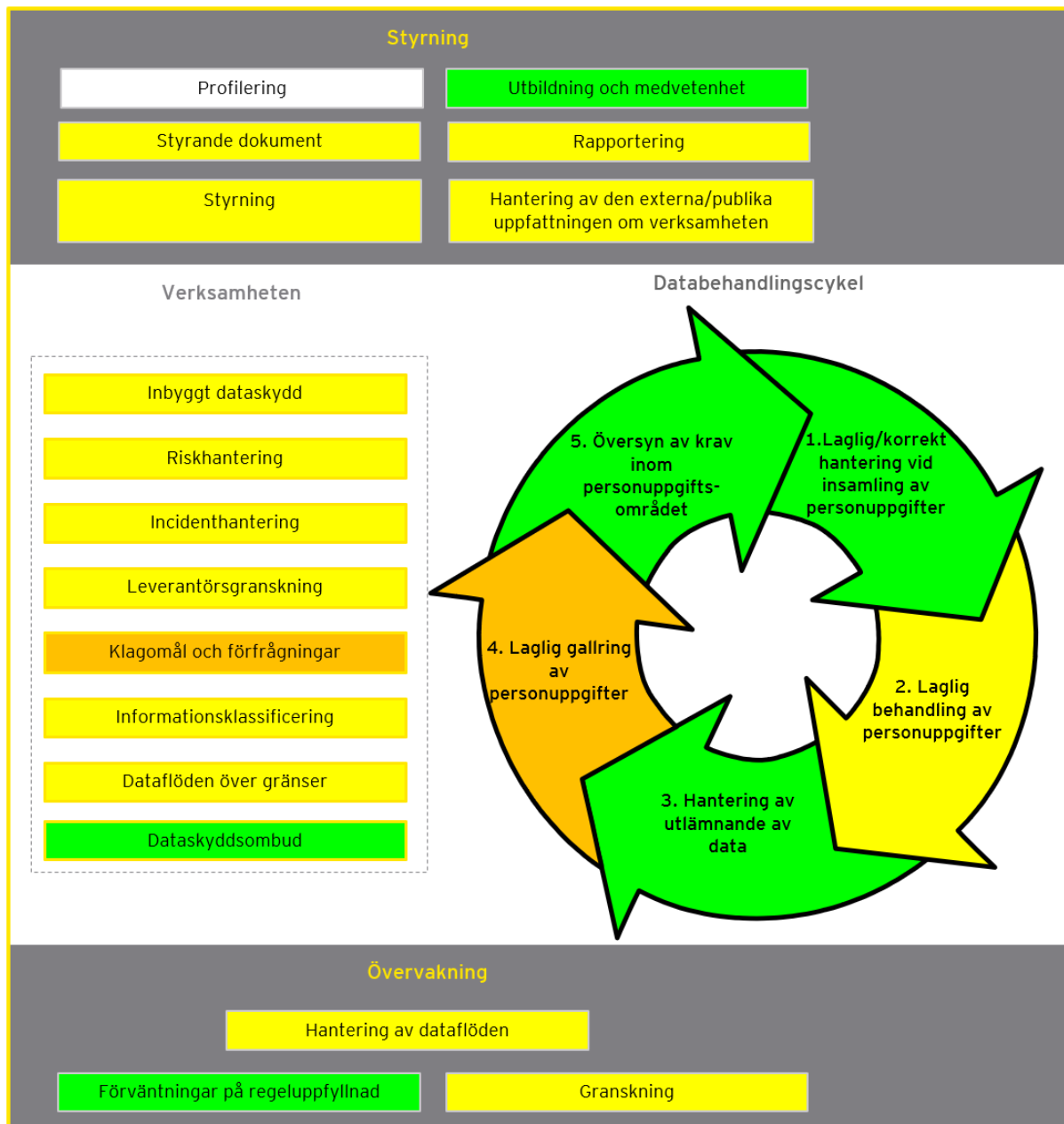
Översiktssbilderna nedan redovisar kommunens mognadsgrad för de 12 huvudområden som granskats, samt nedbrutet på 22 underområden.

Figur 1: Mognadsgrad per område



Nivå 5 representerar hög mognadsgrad och nivå 1 representerar låg mognadsgrad.

Figur 2: Grafisk överblick av mognadsgrad per område. Notera att de 12 huvudområdena är uppdelade i ytterligare detalj.



Mognadsgraden beskrivs enligt den standardiserade skalan med respektive färgkod. De områden som inte var tillämpliga för granskningen är vita.



## 2.1. Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Tabell 1: Observationer inom de 12 områdena

| Område                         | Nuläge   | Iakttagelser  | Mognad |
|--------------------------------|--|---|--------|
| Styrande dokument/<br>styrning | <p>I övergripande reglemente för varje nämnd specificeras att varje nämnd ansvarar för sina egna insamlade personuppgifter och att annan nämnd ska följa den ansvariga nämndens instruktioner vid behandling.</p> <p>Det finns en strategi med övergripande riktlinjer för Nackas arbete med informationssäkerhet. Den är inte anpassad till personuppgiftshantering specifikt eller uppdaterad till de nya kraven som dataskyddsförordningen innebär. Kommunen har prioriterat praktiskt arbete och medvetenhet framför uppdatering av riktlinjer för samtliga processer. Exempelvis pågår ett förbättringsarbete i hur styrning av riskanalys är dokumenterad.</p> <p>Ansvar har fördelats genom delegationsordning för varje nämnd. Kommunfullmäktige har beslutat om att kommunstyrelsen har ett samordningsansvar för dataskydd och informationssäkerhet. Kommunens ansvariga arbetar för att samordna IT- och digitaliseringsfrågor i högre utsträckning än vad som tidigare gjorts. Samtidigt har ansvar och processer aktivt decentraliserats till nämnder och enheter. DSO innehar en nyckelroll för att följa upp efterlevnad, icke-önskade skillnader i dataskyddsarbetet och övriga utmaningar som uppstår vid decentraliserat ansvar och arbete. DSO föreslår åtgärder till varje nämnd genom årlig rapport och har kontinuerligt noga uppsyn över dessas arbete. Nämnder med fler personuppgifter har kommit kortare i implementation, och ingen fastslagen tidsplan finns för att behandla detta.</p> | <p>Ingen uppföljning har gjorts av hur behandlingen av personuppgifter går till i praktiken när en nämnd behandlar personuppgifter där en annan nämnd är personuppgiftsansvarig.</p> <p>Informationssäkerhetsstrategin är inte uppdaterad i enlighet med dataskyddsförordningen. Strukturen på dokumentation från övergripande direktiv till lokala riktlinjer är inte fullt utvecklad eller tydliggjord.</p> <p>I årsrapporterna som DSO presenterar till nämnderna finns det ingen tidsplan för de föreslagna åtgärderna.</p> | 3,0    |

|               |  |  |     |
|---------------|--|--|-----|
| Riskhantering | <p>Nacka har en nyligen uppdaterad mall för konsekvensbedömning. Det finns tydliga direktiv för när och hur denna ska användas, och kartläggning över vilka personuppgifter eller system som behöver genomgå konsekvensbedömning sker eller har skett i samtliga nämnder. Mallen är mycket utförlig och innefattar alla delar som specificeras i dataskyddsförordningen. Det finns ett tydligt samband mellan alla delar av riskhanteringen, från kartläggning till åtgärder. DSO medverkar vanligtvis i processen. Riskanalys och eventuell konsekvensbedömning har dock inte skett för samtliga relevanta fall hittills.</p> <p>Potentiella behov av nya riskbedömningar kan lyftas på veckovisa möten där man diskuterar eventuella förändringar i hanteringen av personuppgifter, men det finns inga fastslagna riktlinjer kring uppdaterade riskanalyser.</p> | <p>Riskanalys och konsekvensbedömning har inte skett för samtliga system eller verksamheter där det är nödvändigt.</p> <p>Det finns ingen plan för uppdaterade riskanalyser vid återkommande intervaller för integritetsrisker i verksamheten och IT-systemen.</p> | 3,8 |
| Kontroll      | <p>DSO är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Nämndernas dataskyddssamordnare har frekvent kontakt med DSO för rådgivning och vägledning.</p> <p>DSO har tagit fram en årlig granskande rapport inkluderande enskilda rapporter för varje nämnd där varje nämnds arbete strukturerat går igenom. Rekommendationer för bättre efterlevnad är inkluderade. Det finns inte dokumenterade rapporteringskrav till kommunledningen eller fastslagen kontrollplan för verksamheten.</p>   | <p>Det finns inga dokumenterade krav på när rapportering till ledning bör ske.</p> <p>Det finns ingen tydligt fastställd internkontrollplan för dataskyddsfrågor.</p>  | 3,2 |

|                                      |   |  |            |
|--------------------------------------|---|--|------------|
| <p>Organisation och ansvar</p>       | <p>Det finns tydlig dokumentation kring organisation och ansvarsfördelning i dataskyddsorganisationen.</p> <p>Kunskapsnivån är mycket god. Resurstilldelningen centralt är mycket god, men det finns utmaningar i nämnderna där informationssäkerhetssamordnarna kan behöva prioritera ned tekniskt informationssäkerhetsarbete på grund av tidsbrist.</p> <p>DSO har en heltidstjänst och jobbar med stöd av jurister och andra experter inom relevanta områden.</p>   |  | <p>4,2</p> |
| <p>Behandling av personuppgifter</p> | <p>Nacka använder sig av systemstödet Draftit som registerförteckning för att hantera personuppgifter. Man har nyligen gått över från sortering på system till sortering på behandling. Totalt i kommunen fanns det vid granskningstillfället 532 behandlingar registrerade i Draftit. Det finns ingen kontroll för att registerförteckningen är helt uppdaterad.</p> <p>Gallring utförs men man har inte granskat att detta sker ändamålsenligt. Därtill saknar man rutiner för att säkerställa att personuppgifter endast behandlas för de ändamål de samlades in för.</p> <p>Kommunens översyn av krav inom området är mycket god.</p> | <p>Det saknas rutiner eller kontroller för att säkerställa registerförteckningens fullständighet och riktighet över tid.</p> <p>Det saknas rutiner eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för och sedan anonymiseras, raderas eller gallras inom rätt tidsram.</p> | <p>3,5</p> |

|                              |  |  |            |
|------------------------------|--|--|------------|
| <p>Val av skyddsåtgärder</p> | <p>Informationsklassning med KLASSA och tillhörande skyddsåtgärder följer efter riskanalysen. DSO är ofta med i processen. Det har inte alltid varit tydligt för ansvariga nämnder när informationsklassning bör ske. DSO har nyligen tydliggjort instruktioner.</p> <p>Kommunen har ett upphandlat avtal med en IT- och informationssäkerhetspartner som man kan avropa konsultstöd från när man upplever att man inte har kapacitet eller kompetens för att driva klassningar själva. Trots detta finns det fortfarande svårigheter att klassificera ostrukturerad information.</p> <p>De centralt ansvariga inom dataskydd har genomfört gedigna utbildningsinsatser för alla medarbetare. Lektioner har skickats ut varannan vecka med kontrollfrågor som kräver eftertanke och kontrollerar att varje anställd går igenom lektionerna. En gång per månad anordnas sittningar med frågor för ansvariga i nämnderna. Det har genomförts regelbundna utbildningar i stadshuset för alla medarbetare som vill lära sig mer. DSO genomför ytterligare utbildningar med dataskyddssamordnare på varje nämnd och enhet där det upplevs att det behövs.</p> | <p>En rutin som säkerställer att samtlig strukturerad information blir klassificerad har inte implementerats.</p> <p>En metod för att genomföra klassificering av ostrukturerad information och dokumentation är inte fullt utvecklad.</p> | <p>3,6</p> |
| <p>Inbyggt dataskydd</p>     | <p>Kommunen har en digitaliseringsenhet som arbetar med utveckling och säkerhetsåtgärder. I guiden för upphandlingar finns krav på vad system behöver uppfylla och innehålla för funktionalitet.</p> <p>Det finns ett utvecklat tänk kring kravet på lagrings- och uppgiftsminimering inom kommunen. Upphandlingar går via en beredningsgrupp som har kompetens inom detta område, och man tar ansvar centralt för att minimera informationslagring i system, till exempel genom att undvika fritextfält i applikationer.</p>  | <p>Kommunen utför begränsade kontroller av behörighetsstrukturer. Det bör som ett minimum finnas rutiner för periodisk granskning av höga behörigheter i känsliga system.</p>  | <p>3,0</p> |

|   |   |   |            |
|---|---|---|------------|
| <p>Hantering av leverantörsrelationer</p> | <p>Kommunen har inventerat alla IT-system som behandlar personuppgifter.</p> <p>Kommunen använder sig av en mall tillhandahållen av SKR för PUB-avtal. PUB-avtal finns med de flesta leverantörer där det är behövligt, och DSO följer upp att arbetet fortgår för de som saknas. Stickprov har visat att det ibland saknas viss information eller bilagor.</p> <p>Avtalen revideras utefter SKR:s revideringar för nya leverantörsavtal. Kommunen funderar på hur man kan kontrollera att biträden följer avtalen. I övrigt finns ingen rutin för att uppdatera avtal eller kontrollera upprätthållandet av dem.</p> <p>Kommunen använder vissa system som har datalagring utanför EU/EES, men dessa innehåller inte känsliga personuppgifter. Det finns rutiner för att inte lagra känsliga personuppgifter ostrukturerat på exempelvis OneDrive.</p> | <p>Det finns inte kompletta PUB-avtal med samtliga leverantörer där det vore relevant.</p> <p>Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.</p> | <p>3,4</p> |
| <p>Hantering av incidenter</p>            | <p>Det finns centrala väldokumenterade rutiner för hur personuppgiftsincidenthantering ska utredas, bedömas, rapporteras och kommuniceras.</p> <p>Varje personuppgiftsansvarig ska upptäcka, utreda, åtgärda och anmäla incidenter. Kontinuerliga utbildningsinsatser har gjort att medarbetarna har hög sannolikhet att korrekt identifiera en incident.</p> <p>Det finns inga etablerade rutiner på plats som kontrollerar att de interna instruktionerna eller rutinerna gällande personuppgiftsincidenter efterlevs.</p>  | <p>En rutin för att granska efterlevnaden av rutinerna gällande personuppgiftsincidenter saknas.</p>  | <p>3,5</p> |

|                                      |  |   |            |
|--------------------------------------|--|---|------------|
| <p>Information till registrerade</p> | <p>Det finns inte dokumenterad styrning för information till registrerade i motsvarande utsträckning som för övriga områden, beroende på att styrdokumentet har utgått från informationssäkerhet generellt och inte uppdaterats till fullo enligt GDPR. Kommunen arbetar med uppdatering av styrdokument.</p> <p>Vid insamling av personuppgifter, lämnas utförlig information till den registrerade om hur personuppgifterna kommer användas.</p> <p>När samtycke används för insamling av personuppgifter används blanketter vars utformning förutsätter att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken. Det är okänt hur samtycket sparas eller hur det kan dras tillbaka.</p> <p>Kommunen bedriver en barnchatt för att stödja barn under pandemin. Det finns även en Facebooksida där kommunen och barn kan nå varandra. Det har nyligen gjorts en konsekvensbedömning för barnchatten. Juridikavdelningen på kommunen har funderat över hur barn ska informeras om sin personuppgiftsbehandling på ett enkelt sätt.</p> | <p>Det finns inte en tydligt dokumenterad väg från styrdokument ner till lokala rutiner för information till registrerade.</p> <p>Det är okänt om en skriftlig rutin som de registrerade kan använda sig av för att ta tillbaka sina samtycken finns eller hur man säkerställer att det i efterhand går att visa att samtycke har samlats in.</p> | <p>3,5</p> |
|--------------------------------------|--|---|------------|

|                                  |   |  |            |
|----------------------------------|---|--|------------|
| <p>Begäran från registrerade</p> | <p>Det finns en kontaktväg via mail och telefon där registrerade kan framföra förfrågningar och klagomål. Det finns utförlig information på hemsidan för de registrerade.</p> <p>Det finns rutiner för hantering av förfrågningar gällande felaktiga, inte längre nödvändiga, eller radering av personuppgifter.</p> <p>Rutinerna för registerutdrag bygger på en tidskrävande manuell process. 2018 observerades det att kvalitetskontroller av denna process skulle vara tidskrävande och kostsamma. Sedan dess har processen justerats för att minska risken för fel. I dagsläget är det en utmaning att få svar i tid från varje enhet när en förfrågan inkommit, och det har inte kontrollerats att enheterna sköter processen korrekt. Det har inte skett några kontroller av att registerutdragen är korrekta.</p> | <p>Det har inte skett kvalitetskontroller av registerutdragen.</p> | <p>2,9</p> |
| <p>Profilering</p>               | <p>Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.</p>   | <p>N/A</p>   | <p>N/A</p> |

## 2.2. Övergripande rekommendationer

*Då flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera fyra övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom förvaltningens dataskydd och informationssäkerhetsarbete.*

### *Kontroll*

Nacka kommun har kommit långt i implementationen av rutiner för säker personuppgiftshantering. Nästa steg för att förbättra verksamheten är utökad kontroll av efterlevnad. Detta kan framförallt ske med centralt förankrade granskningar med tillhörande åtgärdsplaner godkända av ledningen. Dataskyddsombudets årliga granskning är ett bra exempel, men det bör säkerställas att denna, med tillhörande åtgärdsplan, medför tillräckligt eftertryck och precision för att nämnder som ligger efter med dataskyddsarbetet åtgärdar problemen inom rimlig tid. Dessutom kan stickprovstestning utökas och ske oftare för att lättare identifiera brister. Stickprovskontroller skulle behövas för registerförteckning, registerutdrag, gallring, konsekvensanalys, informationsklassning och PUB-avtal. Granskningsresultat bör även kommuniceras till ledningen, exempelvis årligen.

### *Styrande dokument*

Nacka kommun bör säkerställa att alla styrande dokument där så är lämpligt är uppdaterade enligt kraven i dataskyddsförordningen. Kommunen rekommenderas även att se över att styrande dokument och lokala riktlinjer tillsammans bildar en logisk kedja av beslut, ansvarsfördelning och instruktioner som alla medarbetare förstår, så att processerna otvetydigt kan ske i enlighet med vad som är tänkt från centralt håll.

### *Centralisering och effektivitet*

EY rekommenderar att Nacka kommun utvärderar sina processer inom personuppgiftshantering utifrån grad av centralisering och decentralisering för att bedöma om varje process är optimal ur ett resursperspektiv. Nacka har uttryckt att man redan arbetar med detta perspektiv inom digitaliseringsfrågor och tekniska utmaningar, där man genom automatisering och teknisk utveckling både kan öka kontroll och förenkla arbetet. EY rekommenderar att man fortsätter med detta arbete. Nämndernas informationssäkerhetssamordnare kan vara delaktiga för att driva utvecklingen vidare.

### *Begäran från registrerade*

Då processen för registerutdrag är komplex och medför en svårbedömd risk för fel, rekommenderar EY att Nacka kommun prioriterar att kontrollera kvaliteten av utdragen genom exempelvis stickprov. Det kan även vara lämpligt att utvärdera processen för att finna potentiella vägar till förenkling, exempelvis genom att involvera digitaliseringsenheten och undersöka möjligheten för utökad automatisering.



### 3. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av huruvida arbetet kring personuppgiftshantering i Nacka kommun är i enlighet med dataskyddsförordningen. Kommunen bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda, övergripande verksamhet samt karaktär och mängd personuppgiftshantering.

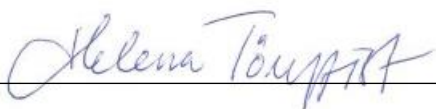
Nacka kommun uppnår mognadsgraden 3,4 av 5,0. Detta är en hög nivå jämfört med vad EY generellt observerar för kommuner, men är samtidigt en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras. Det bör noteras att granskningen gjordes kommunövergripande utan detaljgranskning av de enskilda nämnderna, varför delar i arbetet kan skilja sig mellan olika nämnder.

Kommunen har lagt mycket resurser på arbetet med informationssäkerhet vilket avspeglas i ett omfattande implementationsarbete. Kunskapsnivån inom dataskyddsorganisationen är mycket hög och de ansvariga har genomfört ett gediget arbete med att sprida kunskap i hela kommunen. Organisationen har tagit en riskbaserad ansats för prioriteringar, vilket EY bedömer har bidragit till en ökad mognadsgrad.

Den högsta mognadsgraden observeras således inom organisation och ansvar, utbildning samt riskhantering. Utbildningsinsatser samt metoder för riskanalys och konsekvensbedömning är väl utformade. De lägre mognadsgraderna finns inom styrande dokument, som behöver uppdateras enligt kraven i dataskyddsförordningen och eventuellt utformas tydligare; begäran från registrerade, där risken för felaktigheter fordrar en högre kontroll av efterlevnad; samt inbyggt dataskydd, där man åtminstone bör se över behörighetshanteringen.

Den viktigaste förbättringspunkten anser dock EY är kontroll. För att förbättra implementationen av rutinerna bör det finnas en fastslagen granskningsplan med tillhörande tidsplan för åtgärder. I dagsläget har nämnderna med fler personuppgifter kommit kortare i arbetet, vilket bör prioriteras. Detta kan ske genom en granskning av efterlevnad med tydligare uppföljning och konsekvenser, med åtgärdsplaner godkända av ledningen. Ett praktiskt verktyg för att försäkra sig om att nämnderna arbetar korrekt är att öka mängden stickprov av efterlevnad inom flera kategorier. EY rekommenderar även att kommunledningen fastställer ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till styrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen dokumenteras och rapporteras till ledningsnivå. Detta kan hjälpa kommunen att bedriva ett ändamålsenligt arbete på både kort och lång sikt.

Stockholm den 16 juni 2020



Helena Törnqvist, Partner, EY

## 4. Bilaga 1: Förteckning över intervjuade funktioner

- ▶ Dataskyddsombud
- ▶ Kommunjurist
- ▶ Stadsjurist
- ▶ Digitaliseringschef
- ▶ Stöd- och servicedirektör

## 5. Bilaga 2: Dokumentförteckning

- ▶ Dataskyddsombudets årsrapport 2018
- ▶ Dataskyddsombudets årsrapport 2019
- ▶ Dataskyddsorganisation
- ▶ Delegationsordning för kommunstyrelsen
- ▶ Digitala kortmeddelanden
- ▶ Digitaliseringsstrategi
- ▶ Guide för hantering av personuppgiftsincidenter
- ▶ Guide för lagringsalternativ
- ▶ Guide för säker behörighetshantering
- ▶ Guide för säker e-posthantering
- ▶ Guide för informationsklassning och systemsäkerhetsanalys
- ▶ Guide för informationssäkerhet vid upphandlingar
- ▶ Guide för riskanalys informationssäkerhet
- ▶ Guide och checklista för information till registrerad
- ▶ Informationssäkerhetsstrategi
- ▶ Instruktion för Dataskyddsombud Nacka kommun
- ▶ Instruktion Platina för handläggare av personuppgiftsincidenter
- ▶ Konsekvensbedömning DPIA – mall v 2.1
- ▶ Så här arbetar vi med informationssäkerhet
- ▶ Processkarta incidenthantering
- ▶ Processkarta registerutdrag
- ▶ Reglemente för kommunstyrelsen
- ▶ Mallar från Nackas hemsida:
  - Dataflödesanalys-innehållsbeskrivning
  - Information-registerutdrag-17-maj-2018
  - Instruktion-till-mall-för-personuppgiftsbiträdesavtal
  - Konsekvensbedömning-dpia-instruktion
  - Konsekvensbedömning-dpia-mall
  - Mall-information-till-registrerad-om-personuppgifter
  - PUBA Nacka kommun 20191004
  - Registerutdrag-begaran-om
  - Registerutdrag-infomrationsblad
  - Samtycke-för-behandling-av-personuppgifter

## 6. Bilaga 3: Definitioner

**Behandling:** Med behandling menas varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

**Dataskyddsombud:** Myndigheter och offentliga organ är skyldiga att utse dataskyddsombud. Dataskyddsombudets uppgifter är bland annat att informera och ge råd inom den egna organisationen om vilka skyldigheter som gäller enligt såväl förordningen som nationella bestämmelser. Ombudet ska också bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen. Slutligen ska ombudet fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna.

**EU/EES:** EU står för den Europeiska unionen och EES för Europeiska ekonomiska samarbetsområdet. I EU ingår följande länder Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Förenade Kungariket, Grekland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern, Österrike. I EES ingår utöver länderna i EU även Island, Liechtenstein och Norge.

**Förhandssamråd:** Om man vid en konsekvensbedömning bedömer att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken måste man samråda med Datainspektionen.

**Informationsklassning:** Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

**Informationssäkerhet:** Berör i huvudsak säkerhetsfrågor som berör information, oberoende av system, eller plattformar.

**Konsekvensanalys:** Innan man inleder en behandling av personuppgifter som kan leda till en hög risk för integritetsintrång till exempel ett omfattande register med känsliga personuppgifter, måste man bedöma konsekvenserna för de registrerade (konsekvensbedömning).

**Känslig personuppgift:** Exempel på känsliga personuppgifter är ras och etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, biometriska och genetiska data, medlemskap i fackförening, hälsa eller uppgifter om fysisk persons sexualliv eller sexuell läggning.

**Personuppgift:** Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk levande person, d.v.s. medborgare, anställda m.fl. Exempel på personuppgifter är namn, personnummer, telefonnummer, bank- och kontouppgifter, IP-adress, försäkringsnummer m.m.

**Personuppgiftsansvarig:** Med personuppgiftsansvarig avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

**Personuppgiftsbiträde:** Med personuppgiftsbiträde avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för personuppgiftsansvarigs räkning.

**Personuppgiftsincident:** En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

**Policy och instruktion:** Avser dokumentation av rutiner på ett eller annat sätt. I denna rapporten görs ingen skillnad på om dokumentationen är antagen på politisk eller tjänstemannanivå.

**Profilerig:** Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

**Pseudonymisering:** Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. De kompletterande uppgifterna ska förvaras separat och vara föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

**Register:** En strukturerad samling av samtliga personuppgiftsbehandlingar som företas inom verksamheten.

**Registrerad:** Med registrerad avses den enskilde vars personuppgifter behandlas.

**Samtycke:** Med samtycke avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring från den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

**Tillsynsmyndighet:** En oberoende offentlig myndighet som är utsedd av en medlemsstat. I Sverige är Datainspektionen tillsynsmyndighet.

**Tredje land:** Med tredje land avses ett land som inte är medlem i EU eller EES. En överföring till tredje land är när personuppgifter som behandlas i ett EU- eller EES-land görs tillgängliga i ett land utanför EU/EES-området. Exempelvis när personuppgifter i ett datoriserat register skrivs ut och skickas i pappersform eller när personuppgifter skickas via e-post. Personuppgifter får föras över endast om det finns en adekvat skyddsnivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de registrerades rättigheter skyddas.

**Tredje part:** Med tredje part avses en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige,

personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna.