Södertälje kommun

Revisorerna

Revisionsskrivelse

2021-06-09

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Revisionsrapport nr 3/2021 – Granskning efterlevnad av dataskyddsförordningen (GDPR)

På vårt uppdrag har EY genomfört en granskning av kommunens hantering av personuppgifter kopplat mot de krav som införts genom dataskyddsförordningens (GDPR) ikraftträdande den 25 maj 2018. Personuppgiftsbehandling sker i så gott som alla delar av den kommunala organisationen, men särskilt mycket känsliga uppgifter hanteras i social-, omsorgs- och utbildningskontoren.

Den övergripande bedömningen är att Södertälje kommun har en genomsnittlig mognadsgrad, jämfört med andra kommuner av liknande storlek och karaktär. Då den generella mognaden inom kommunal sektor är låg innebär detta dock att det finns brister i efterlevnaden av dataskyddsförordningen. Granskningen har därutöver noterat att kommunen arbetar ambitiöst med personuppgiftsfrågor och nyckelpersonerna i den centrala dataskyddsorganisationen har varit strakt bidragande i detta arbete.

Sammanfattningsvis visar granskningen att det finns ett antal brister och utvecklingsområden som resulterar i rekommendationer, vilka vi instämmer i.

Svar från kommunstyrelsen, önskas senast 2021-09-30.

För revisorerna i Södertälje kommun

Christer Björk Elisabet Komheden

Bilaga: Revisionsrapport nr 3/2021 – Granskning efterlevnad av dataskyddsförordningen (GDPR)

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

CHRISTER BJÖRK
Undertecknare 1
Serienummer: 19460420xxxx
IP: 90.224.xxx.xxx
2021-06-11 12:32:16Z

BankID

ELISABET KOMHEDEN
Undertecknare 2
Serienummer: 19540522xxxx
IP: 213.67.xxx.xxx
2021-06-11 12:44:09Z

BankID

Granskning efterlevnad av
dataskyddsförordningen (GDPR)
På uppdrag av de förtroendevalda revisorerna
Södertälje kommun

Södertälje kommun

Granskning av efterlevnad dataskyddsförordningen (GDPR), juni 2021

Building a better working world

Ernst & Young AB
111 47 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Building a better working world

Sammanfattning

EY har på uppdrag av Södertälje kommuns förtroendevalda revisorer genomfört en granskning av kommunen, samt dess nämnder och förvaltningar (förvaltningar hänvisas hädanefter till begreppet "kontor" baserat på vad som används inom kommunen), med avseende på personuppgiftshantering.

Granskningens syfte har varit att ge en *övergripande* förståelse av huruvida Södertälje kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) 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 mars 2021 till juni 2021. Enligt metoden bedöms kommunens 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 Södertälje kommun ha den genomsnittliga mognadsgraden 2,73 av 5,0. Detta är en genomsnittlig mognadsgrad om man jämför med vad EY har observerat i andra kommuner av liknande storlek. Samtidigt är det en lägre mognadsgrad än vad EY rekommenderar för en kommun, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningarna. Södertälje har arbetat ambitiöst med personuppgiftsfrågor och nyckelpersonerna i den centrala dataskyddsorganisationen har kommit långt i sitt arbete.

Överlag bedöms mognadsgraden vara högst inom hantering av incidenter, organisation och ansvar samt begäran från registrerade. Inom kommunen arbetar de personer som är ansvariga för informationssäkerhet och personuppgiftshantering ambitiöst med integritetsfrågor samt dataskydd, och man uppvisar en stor förståelse samt en god kunskap för dataskyddsförordningen och dess krav. I dagsläget finns det en tydlig ansvarsfördelning kring dataskyddsarbetet inom kommunen, och man påvisar även ambitioner att fortsätta utveckla verksamhetens dataskyddsorganisation för att skapa en förbättrad samordning av arbetet med personuppgifter.

Den viktigaste förbättringspunkten som EY rekommenderar 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 också att kommunen jobbar vidare inom området utbildning och medvetenhet, samt med rutinerna för att genomföra konsekvensbedömningar på befintliga personuppgiftsbehandlingar.

Ernst & Young AB
111 47 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Innehållsförteckning

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. Bakgrund

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 uppdagats.
- Individer har rätt till ersättning i form av skadestånd till följd av överträdelser av förordningen av en personuppgiftsansvarig eller ett personuppgiftsbiträde.

Integritetsskyddsmyndigheten (IMY) är den tillsynsmyndighet som ansvarar för uppföljning och kontroll av att lag och förordning efterlevs. I oktober 2018 publicerade Integritetsskyddsmyndigheten en "sammanställning av resultatet från granskning av dataskyddsombud". 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. Integritetsskyddsmyndigheten har också inlett andra inspektioner inom ramen för dataskyddsförordningens efterlevnad.

Då Södertälje kommun med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna i Södertälje kommun beslutat att genomföra en helhetsgranskning av kommunens arbete med personuppgiftshantering med hänsyn till dataskyddsförordningen (GDPR).

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1.2. Syfte och revisionsfrågor

Syftet med granskningen är att ge en *övergripande* förståelse av huruvida Södertälje kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar. Granskningen ska svara på följande tre revisionsfrågor:

- *Arbetar* Södertälje kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Södertälje kommuns *policyer och riktlinjer* ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Södertälje kommun ändamålsenlig *kontroll och uppföljning* av arbetet med dataskyddsförordningen (GDPR)?

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 Södertälje kommun bedriver på central nivå och inga av kommunens kontor har således granskats i ytterligare detalj. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

1.4. Metod

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete samt genomgång av relevant dokumentation (se *Bilaga 2: Dokumentförteckning*). Granskningen är utförd mot 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. 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. Besvarandet av frågorna som innefattas av ramverket sker genom möten 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.

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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. Profilering

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 till exempel ett område med grön färgkod ändå sakna viktiga kontroller. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Inledningsvis har underlag såsom policyer, strategi- och styrdokument och dylikt samlats in för att analyseras. Därefter höll EY:s GDPR-specialister ett arbetsmöte med ansvariga inom kommunen (se *Bilaga 1: Förteckning över intervjuade funktioner*). Under detta arbetsmöte avhandlades samtliga 12 områden. Efter att EY analyserat resultatet av mötet 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:

- Mars 2021 – Förberedelser, planering och insamling av dokumentation.
- Mars 2021 – Maj 2021 – Dokumentanalys, utförande av ett arbetsmöte (2021-03-30), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport samt faktagranskning av kommunen.
- Juni 2021 – Kvalitetssäkring av EYs verksamhetsrevisorer och slutgiltig presentation för kommunens förtroendevalda revisorer.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

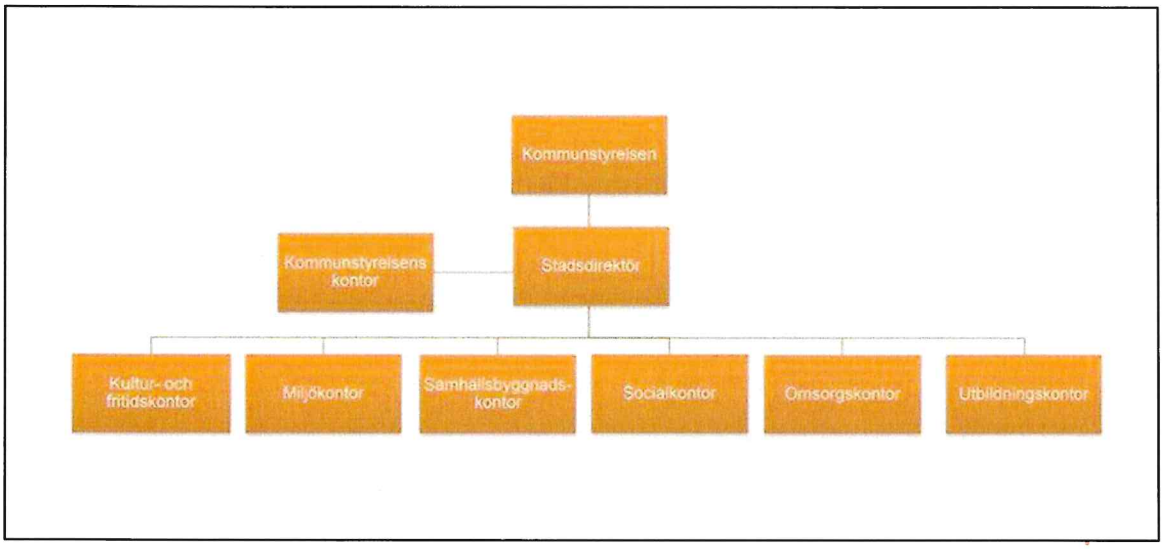
Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1.5. Definitioner

Se bilaga 3.

1.6. Organisationsstruktur

Figur 1: Organisationsschema – Förvaltningens organisation. Hämtad från Södertälje kommuns hemsida 2021-05-26.



Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2. Analys

Baserat på utförd granskning konstaterades det att Södertälje kommun på en central nivå ligger på en genomsnittlig mognadsgrad i jämförelse med det EY generellt sett observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Kommunens genomsnittliga mognadsgrad uppnår en summa av 2,73, vilket är en lägre mognadsgrad än vad EY rekommenderar för en kommun, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras av Södertälje kommun.

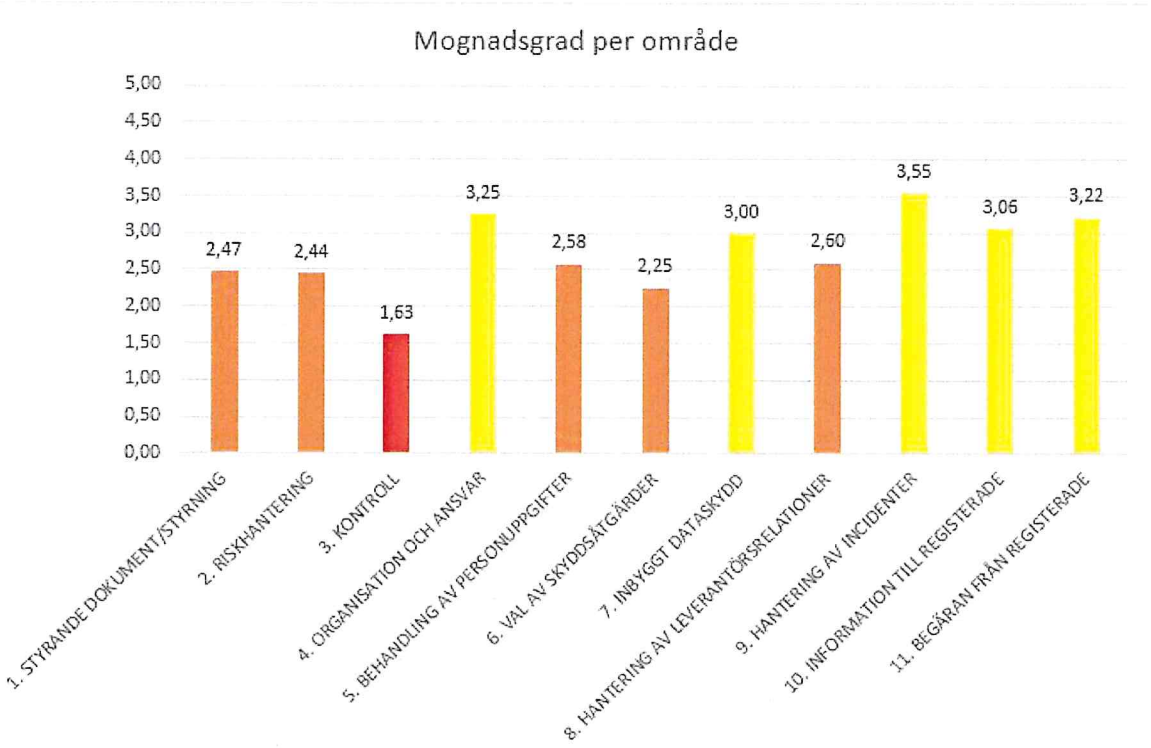
Inom kommunen arbetar de personer som är ansvariga för informationssäkerhet och personuppgiftshantering ambitiöst med integritetsfrågor samt dataskydd, och man visar inom kommunen en stor förståelse samt en god kunskap för dataskyddsförordningen och dess krav. I dagsläget finns det en tydlig ansvarsfördelning kring dataskyddsarbetet inom kommunen, och man påvisar även ambitioner att fortsätta utveckla verksamhetens dataskyddsorganisation för att skapa en förbättrad samordning av arbetet med personuppgifter.

Det finns ett antal identifierade utvecklingsområden för Södertälje kommun att vidareutveckla inom personuppgiftshantering. Kommunen saknar i dagsläget ett centraliserat arbete med personuppgifter som är samordnat mellan kommunens verksamheter, men man har påbörjat arbetet med att etablera en ny dataskyddsorganisation med syftet att öka centralisering samt samverkan. Styrningen från kommunstyrelsen är inte komplett då man exempelvis inte har etablerat en rutin för att granska verksamheternas arbete med personuppgifter eller ställt krav på kontinuerlig rapportering från respektive förvaltning till central nivå. Det finns även en utvecklingspotential inom området utbildning och medvetenhet inom Södertälje kommun, samt inom rutinerna för att genomföra konsekvensbedömningar på befintliga personuppgiftsbehandlingar.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Figur 2: Mognadsgrad per område

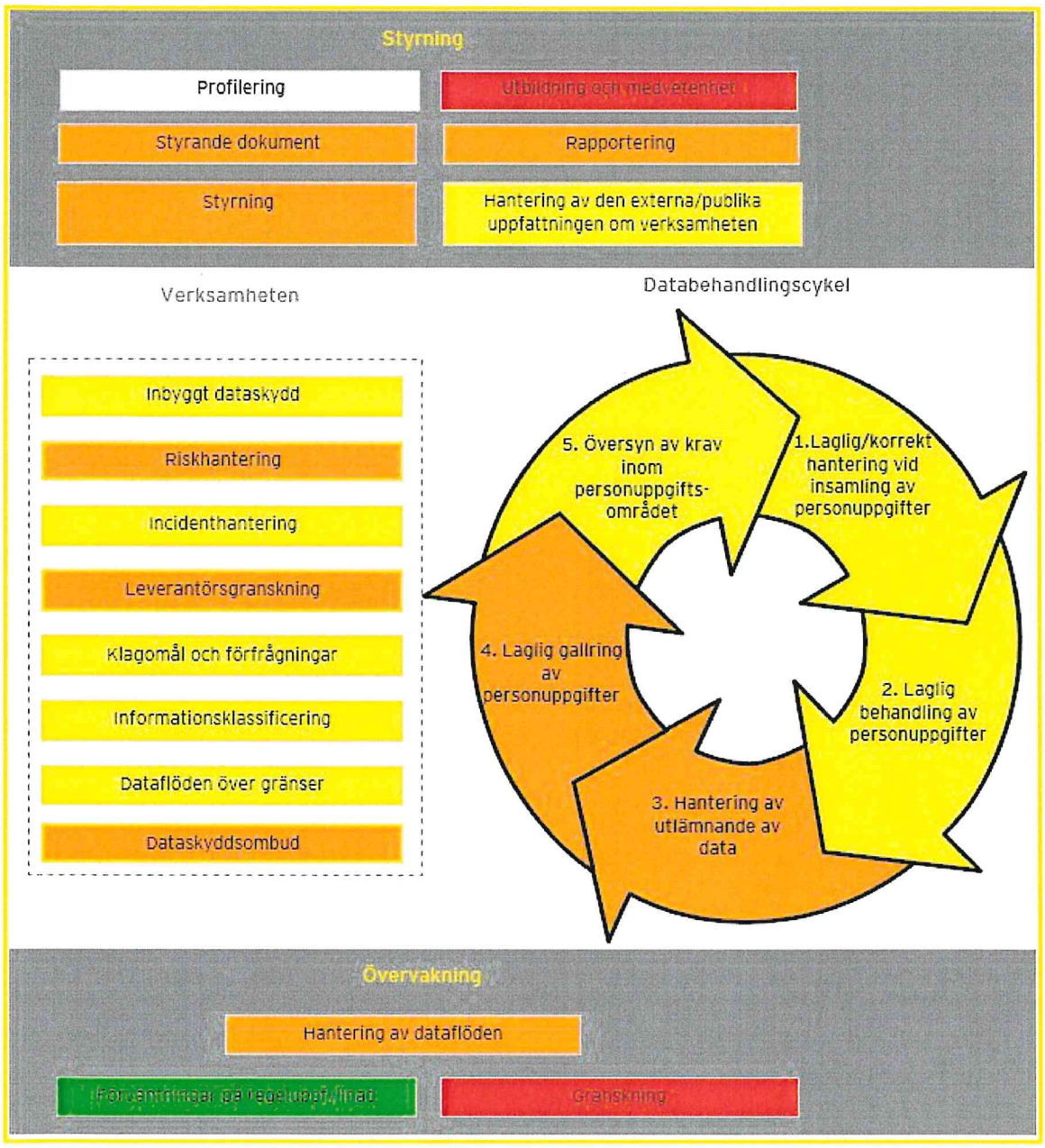


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

Figur 3: Grafisk överblick av mognadsgrad per område (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873



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

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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/ styrning	Södertälje kommun har en policy för informationssäkerhet som uttrycker kommunstyrelsens övergripande viljeriktning för kommunens arbete med informationssäkerhet. Kommunens nämnder är personuppgiftsansvariga för deras verksamheter och ska följa kommungemensamma policyer, samt ansvarar för efterlevnaden av dessa i respektive verksamhet. Informationssäkerhetspolicyn reviderades senast under 2020. Informationssäkerhetsansvarig på kommunen ansvarar för uppföljning av policyn, samt för att revidera policyn vid behov. Det finns i dagsläget inga fastställda rutiner för att kontinuerligt granska samt uppdatera policyn. Det finns ett kommungemensamt styrdokument för hanteringen av personuppgifter inom kommunen, fastställt av kommunstyrelsen 2019. Man har inte reviderat dessa riktlinjer sedan de fastställdes. Kommunen har haft en målsättning att löpande följa upp samt arbeta vidare med riktlinjerna för personuppgiftshantering, med ambitionen att utifrån dessa ta fram lokala instruktioner för varje enskild verksamhet. Då detta ännu inte har genomförts, saknas det rutiner för hur informationssäkerhet samt personuppgiftshantering omsätts i praktiken i respektive verksamhet. Södertälje kommun har påbörjat arbetet med en ny dataskyddsorganisation, med syftet att centralisera kommunens arbete med personuppgifter och skapa en samverkan mellan alla verksamheter. Med hjälp av detta initiativ hoppas man att varje enskild verksamhet ska få tillräckligt stöd för att genomföra ett adekvat arbete med personuppgiftshantering.	Det saknas formella rutiner för att kontinuerligt granska samt uppdatera styrande dokument relaterade till informationssäkerhet och personuppgiftshantering. Det finns inga lokala instruktioner för respektive verksamhet beträffande hantering av personuppgifter som fastställer hur styrande riktlinjer omsätts samt efterlevs i praktiken.	2,47

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Riskhantering	Det finns en kommungemensam riktlinje för hur kommunens verksamheter ska arbeta med riskbedömning samt riskhantering vid anskaffning, införande eller användning av ett verksamhetsstöd. Riktlinjen påvisar att kommunen har en utarbetad metod för att genomföra adekvata risk- samt sårbarhetsanalyser. Man har en ambition att använda denna metod för att bedöma risker som kan finnas i samband med personuppgiftshantering, men det är inget som kontinuerligt sker i dagsläget. Kommunen använder sig av en tröskelanalys för att avgöra om en konsekvensbedömning är nödvändig, och om så är fallet att genomföra dessa, i enlighet med metoden kallad Data Protection Impact Assessment (DPIA). Metoden används främst inför nya personuppgiftsbehandlingar. Det saknas dock en rutin för att säkerställa att konsekvensbedömningar genomförs kontinuerligt för samtliga nya samt befintliga behandlingar.	Det saknas formella rutiner samt krav för att kontinuerligt inkludera integritetsrisker i kommunens arbete med riskanalyser. Konsekvensbedömningar genomförs inte löpande för samtliga behandlingar där det vore nödvändigt.	2,44
Kontroll	Kommunen har utsett sitt kommungemensamma dataskyddsombud (DSO) som kontaktperson gentemot Integritetsskyddsmyndigheten på central nivå. Då respektive verksamhet inom kommunen har en dataskyddssamordnare (DSS), är dessa utsedda kontaktpersoner gentemot Integritetsskyddsmyndigheten på verksamhetsnivå. Det finns informella rutiner för hur exempelvis en incidentanmälan ska göras till tillsynsmyndighet i respektive verksamhet, men det finns ingen formell rutin på central nivå för hur man ska bistå Integritetsskyddsmyndigheten med efterfrågad information. DSO har kontinuerlig kontakt med respektive DSS, men kommunens verksamheter saknar i dagsläget formella rutiner för att rapportera till kommunstyrelsen om status för dataskyddsarbetet, exempelvis rapportering av personuppgiftsincidenter. Man har tidigare arbetat med löpande rapportering inom verksamheten, men det är inte längre något som genomförs. Södertälje kommun saknar en fastslagen granskningsplan alternativt internkontrollplan för att utvärdera samt säkerställa att man uppfyller relevanta krav på hantering av personlig information inom kommunens respektive verksamheter.	Det saknas formella rutiner för att rapportera till, samt svara på, förfrågningar från Integritetsskyddsmyndigheten. En formell rutin för rapportering från respektive verksamhet till kommunstyrelse, samt krav som sådan rapportering ska utgå ifrån, har inte förankrats. Det finns ingen fastslagen granskningsplan eller internkontrollfunktion som följer upp att kommunens verksamheter hanterar personuppgifter i enlighet med dataskyddsförordningen.	1,63

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Organisation och ansvar	Södertälje kommun har en tydlig dokumentation kring organisation samt ansvarsfördelning inom sin dataskyddsorganisation. I denna uttrycks även målsättning att framöver utveckla sin samverkan inom kommunen kring arbetet med personuppgifter. Kunskapsnivån kring dataskyddsförordningens krav, samt Integritetsskyddsmyndighetens befogenheter, är god inom kommunen. Kommunen har i dagsläget ett kommungemensamt dataskyddsombud (DSO) som huvudsakligen arbetar med uppgifter relaterade till en annan roll i verksamheten. Då DSO genomför operativt arbete finns det vissa intressekonflikter, eftersom DSO till viss del granskar arbetet denne själv har implementerat. Verksamheten är medveten om denna problematik och planerar att anställa en extern, kommungemensam DSO i samband med implementationen av deras nya dataskyddsorganisation för att säkerställa en oberoende granskning. Varje enskild verksamhet inom kommunen har en dataskyddssamordnare (DSS) som ska samordna arbetet med personuppgiftshantering i respektive verksamhet. Kommunen planerar att upprätta en ny kommungemensam tjänst som dataskyddskoordinator (DSK), med syftet att stötta och samordna respektive DSS arbete.	Kommunen har inte säkerställt att DSO enbart har en rådgivande position, utan DSO granskar även till viss del arbetet denne har implementerat.	3,25
Behandling av person-uppgifter	Södertälje kommun använder sig av ett systemverktyg för att upprätthålla en registerförteckning i enlighet med dataskyddsförordningens krav. Registerförteckningen innehåller alla kommunens behandlingar, samt en förteckning över kommunens IT-system. Det är respektive dataskyddssamordnares (DSS) ansvar att uppdatera registerförteckningen för deras verksamhet, vilket sker genom ett löpande informellt arbete då det saknas formella rutiner för hur detta ska genomföras. Det finns en dokumenthanteringsplan som omfattar riktlinjer för gallring av personuppgifter. Dokumenthanteringsplanen anger vilka tidsgränser som gäller för gallringen. I dagsläget genomför man inga kontroller för att säkerställa att gallring genomförs i praktiken. Det finns en löpande kommunikation mellan varje DSS och medarbetare i deras verksamheter kring vilka personuppgifter som får samlas in för att säkerställa dess rätta ändamål, men det finns inga formella rutiner för detta.	Det saknas formella rutiner eller kontroller för att säkerställa registerförteckningens fullständighet och riktighet över tid. Det saknas rutiner och/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.	2,58

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Val av skydds-åtgärder	Södertälje kommun använder sig av SKR:s verktyg KLASSA för att klassificera verksamhetens IT-system samt ta fram tillhörande skyddsåtgärder utifrån dataskyddsförordningens krav. Det finns i dagsläget ingen metod eller rutin för att genomföra klassificering av ostrukturerad information. Via kommunens intranät distribueras information kring dataskydd- samt integritetsfrågor till anställda. Det hålls inga obligatoriska utbildningar för att kontinuerligt skapa en medvetenhet om vikten av, samt de anställdas ansvar när det gäller integritet samt dataskydd. Kommunen arbetar i dagsläget för att ta fram en grundutbildning inom dataskyddsförordningen som ska omfatta separata utbildningstillfällen för respektive kontor.	En metod och rutin för att genomföra klassificering av ostrukturerad information saknas. Kommunen genomför inte regelbundna utbildningar med anställda inom dataskyddsförordningen.	2,25
Inbyggt dataskydd	Kommunen har tagit fram en intern riktlinje för inbyggt dataskydd vid upphandling av nya IT-system, som grundar sig i dataskyddsförordningens krav. En viss informell behörighetshantering genomförs inom verksamheten, då systemförvaltare kontinuerligt arbetar med att kontrollera vilka behörigheter som finns i deras IT-system. Det finns ingen formell rutin eller riktlinje för hur man ska arbeta med behörighetsstrukturer inom kommunen. Det finns en medvetenhet inom kommunen kring behörighetsstrukturer då man i den operativa verksamheten har upptäckt att äldre behörigheter som borde ha tagits bort i vissa fall kvarstår.	Kommunen utför begränsade kontroller av behörighetsstrukturer. Det bör som ett minimum finnas rutiner för periodisk granskning av höga behörigheter i känsliga system.	3,0

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Hantering av leverantörs-relationer	Södertälje kommun använder sig av en mall för PUB-avtal framtagen av SKR. Kommunen har ett inköpsbolag som hanterar verksamhetens upphandlingar, där PUB-avtal alltid ska ingå vid nya upphandlingar. PUB-avtal finns med de flesta leverantörer där det är behövligt, men man har inte genomfört någon granskning för att säkerställa att det finns PUB-avtal med samtliga leverantörer där det vore relevant. Det finns även kommungemensamma riktlinjer samt instruktioner för vad respektive verksamhet i kommunen bör tänka på vid upprättandet av ett PUB-avtal. Man har diskuterat att genomföra leverantörsgranskningar exempelvis i form av stickprov för att säkerställa att leverantörer lever upp till kraven i dataskyddsförordningen över tid, men det är inget som genomförs i dagsläget. Underleverantörer måste godkännas av kommunen, samt eventuella personuppgiftsincidenter hos leverantörer och underleverantörer ska rapporteras till kommunen enligt krav i PUB-avtalen. Kommunen använder vissa system som har datalagring utanför EU/EES, men dessa innehåller inte några känsliga personuppgifter. Det finns vissa rutiner för att hantera datalagring utanför EU/EES, exempelvis med hjälp av kryptering.	Det finns inte PUB-avtal med vissa leverantörer där det vore relevant. Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.	2,60
Hantering av incidenter	Södertälje kommun har tagit fram centrala väldokumenterade instruktioner samt riktlinjer för hur en personuppgiftsincident ska utredas, bedömas, rapporteras samt kommuniceras. Detta inkluderar även hur man ska informera berörda registrerade vid en eventuell personuppgiftsincident. Via en e-tjänst på kommunens intranät ska anställda som misstänker att en personuppgiftsincident har skett anmäla detta. Vid en anmäld incident informeras kommunens dataskyddsombud (DSO) samt respektive dataskyddssamordnare (DSS) via e-mail, som gör en gemensam bedömning av incidentens allvarlighetsgrad och tar ett beslut om incidenten ska rapporteras till Integritetsskyddsmyndigheten. Alla anmälda personuppgiftsincidenter lagras i kommunens e-tjänst. I dagsläget finns det inga formella rutiner för att granska huruvida de interna instruktionerna gällande personuppgiftsincidenter efterlevs i praktiken.		3,55

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Information till registrerade	Vid insamling av personuppgifter lämnas utförlig information till den registrerade om hur personuppgifterna kommer att användas. Via Södertäljes kommun finns det även utförlig information till de registrerade kring hur deras personuppgifter ska behandlas av kommunen samt vilka rättigheter den registrerade har. Verksamheten använder samtycke som laglig grund relativt sällan, och då främst i form av foton som ska användas i marknadsföringssyfte på kommunens olika kanaler. Man har tagit fram en samtyckesblankett som säkerställer att samtycket bygger på en aktiv handling samt är distinkt, tydligt och inte ihopblandat med andra samtycken. Registrerade kan även lämna sitt samtycke via kommunens e-tjänst. Det finns inte någon formellt dokumenterad rutin för hur kommunen ska kommunicera med de registrerade vid eventuella förändringar i hur de behandlar personuppgifter.	Det saknas en process för hur kommunen kommunicerar möjliga förändringar i hur man hanterar personuppgifter till de registrerade.	3,06
Begäran från registrerade	På Södertälje kommuns hemsida finns en tydlig kontaktväg där registrerade via e-mail kan framföra förfrågningar samt eventuella klagomål. Kommunen har tagit fram en intern rutin för att hantera förfrågningar från registrerade av registerutdrag. Rutinen omfattar de registrerades rättigheter i enlighet med dataskyddsförordningen, det vill säga information, tillgång, rättelse, radering, samt begränsning av personuppgifter. Rutinen innehåller även dokumenterade processflöden för hur en begäran ska hanteras. Kommunen har inte genomfört några interna kvalitetskontroller, exempelvis stickprov, av registerutdragen. Registrerade kan använda sig av kommunens e-tjänst för att genomföra en begäran, och identifierar sig då med hjälp av bank-id. Om en registrerad besöker kommunens kontaktcenter, kräver kommunen att den registrerade ska kunna visa legitimation vid tillfället denne gör en begäran.	Det har inte skett några kvalitetskontroller av registerutdragen.	3,22
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.	N/A	N/A

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2.2. Övergripande rekommendationer

Då iakttagelser har identifierats inom flera delar av ramverket har EY valt att presentera fyra övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom Södertälje kommuns dataskydd och informationssäkerhetsarbete. Rekommendationerna är rangordnade i prioritetsordning men EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Granskning och rapportering

En begränsad uppföljning av informationssäkerhetsarbetet i kommunens verksamheter medför en risk att den dagliga informationshanteringen i respektive kontor avviker från det sätt som kommunen anvisar samt tror att arbetet bedrivs på. Då det i dagsläget inte finns någon etablerad rapportering kring personuppgiftsarbetet i respektive kontor, eller någon uppföljande granskning från kommunstyrelsens sida, rekommenderas kommunen att implementera en granskningsplan för arbetet med personuppgifter i verksamheten. Granskningsplanen kan användas för att utvärdera och säkerställa att man inom kommunen uppfyller relevanta krav på hantering av personlig information. Exempelvis skulle granskningsplanen kunna generera kontroller av kommunens dataskyddsarbete som integreras med deras befintliga internkontrollarbete. Slutligen, rekommenderas även kommunen att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapportering till kommunstyrelse kan utgå från för att säkerställa att uppföljning av arbetet med dataskyddsförordningen i kommunen utförs och kontinuerligt kommuniceras till ledningen.

Utbildning & medvetenhet

En bristfällig kommunikation av policyer, anvisningar samt instruktioner gällande informationssäkerhet kan medföra en risk att kommunens medarbetare besitter en otillräcklig kunskap för att på daglig basis hantera verksamhetens information på ett säkert samt ändamålsenligt sätt. Kommunen rekommenderas därmed att införa vidareutbildningar inom integritet och dataskydd för samtliga medarbetare. Utbildningar inom personuppgiftshantering rekommenderas att genomföras med en bestämd frekvens samt med en viss uppföljning, för att säkerställa att alla medarbetare tagit del av utbildningarna. Utbildningarna bör regelbundet uppdateras för att säkerställa att nya krav och förhållningssätt kommuniceras till samtliga medarbetare.

Styrning och styrande dokument

Södertälje kommun rekommenderas att fortsätta driva arbetet med att ta fram lokala instruktioner för personuppgiftshantering för respektive verksamhet, för att säkerställa att deras policy för informationssäkerhet samt kommungemensamma riktlinjer för personuppgiftshantering konkretiseras och efterlevs i praktiken. Vidare rekommenderas kommunen att genom detta arbete se till att det bildas en logisk kedja av beslut, ansvarsfördelning samt instruktioner som samtliga medarbetare förstår, så att processerna otvetydigt kan ske i enlighet med vad som är tänkt från centralt håll. Slutligen rekommenderas kommunen att införa tydligare rutiner för att kontinuerligt granska samt uppdatera deras styrdokument kring informationssäkerhet samt personuppgiftshantering, för att säkerställa dess aktualitet till rådande lagstiftning.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Riskhantering

Riskhantering syftar till att utvärdera hur verksamheten identifierar samt minskar integritetsrisker i sin verksamhet och dess IT-system. Kommunen har väldokumenterade rutiner för hur både risk- samt konsekvensbedömningar ska genomföras inom verksamheten, men då det finns vissa tveksamheter kring hur dessa efterlevs i praktiken rekommenderas kommunen att vidareutveckla dessa rutiner samt ta fram en ansvarsfördelning för att säkerställa att risk- samt konsekvensbedömningar genomförs vid återkommande intervaller. Vidare rekommenderas kommunen att se över sina rutiner för att genomföra konsekvensbedömningar även på befintliga personuppgiftsbehandlingar, för att säkerställa att man minimerar nya eller förändrade risker kopplade till sitt arbete med personuppgifter.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Revisionsfrågor

Revisionsfrågorna besvaras utifrån granskningen som helhet, det vill säga Södertälje kommuns kommunala verksamheter.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Arbetar Södertälje kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?	Södertälje kommun bedöms delvis arbeta ändamålsenligt för att uppfylla de krav och regleringar som införts i och med dataskyddsförordningen (GDPR). Svaret baserar sig främst på att kommunen uppvisar stor kunskap samt höga ambitioner inom arbetet med dataskyddsförordningen. Mognadsgraden beskrivs vidare som genomsnittlig i jämförelse med kommuner av liknande storlek. Det återstår dock vissa komponenter innan arbetet kan beskrivas som ändamålsenligt, exempelvis implementera rutiner för kontroll och uppföljning.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Är Södertälje kommuns policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?	Södertälje kommuns policyer, riktlinjer och instruktioner bedöms delvis vara ändamålsenligt för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR). Södertälje kommun har skapat många relevant policyer, riktlinjer samt instruktioner som används genomgående i kommunens arbete med dataskyddsförordningen. Det finns dock fortfarande vissa relevanta riktlinjer och instruktioner som inte har tagits fram än, exempelvis kring utbildning, konsekvensbedömningar samt lokala instruktioner för att säkerställa att centrala rutiner efterlevs. Kommunen behöver dessutom jobba vidare med att säkerställa att policyer, rutiner och instruktioner kontinuerligt hålls uppdaterade.	
Har Södertälje kommun ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?	Södertälje kommun bedöms inte ha en ändamålsenlig kontroll och uppföljning med avseende på dataskyddsförordningen (GDPR). Svaret baseras på att Södertälje kommun inte genomför kontroll och uppföljning på kommunövergripande nivå och att det saknas en strukturerad granskningsplan. Det finns heller inga dokumenterade rutiner för uppföljning på verksamhetsnivå och således sker ingen rapportering kring uppföljning och efterlevnad.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Slutsatser

Syftet med granskningen har varit att undersöka huruvida Södertälje kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen. Detta syfte har besvarats med hjälp av tre revisionsfrågor:

- *Arbetar* Södertälje kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Södertälje kommuns *policyer och riktlinjer* ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Södertälje kommun ändamålsenlig *kontroll och uppföljning* av arbetet med dataskyddsförordningen (GDPR)?

I besvarandet av dessa revisionsfrågor bedöms kommunen i relation till andra kommuner och offentliga organisationer av liknande storlek och karaktär. EY:s övergripande bedömning är att Södertälje kommun till största delen bedriver ett ändamålsenligt arbete för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen. Kommunen rekommenderas dock att arbeta vidare med att säkerställa att samtliga relevanta policyer, rutiner och instruktioner finns på plats samt att implementera en granskningsplan för arbetet med personuppgifter i verksamheten och på så sätt säkerställa ändamålsenlig kontroll och uppföljning.

Södertälje kommun har en genomsnittlig mognadsgrad i jämförelse med andra kommuner och offentliga organisationer av liknande storlek och karaktär, med ett snitt på 2,73 på en femgradig skala. Det är dock en lägre mognadsgrad än vad EY rekommenderar för en kommun, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom organisationen. Överlag bedöms mognadsgraden vara högst inom hantering av incidenter, organisation och ansvar samt begäran från registrerade. Inom kommunen arbetar de personer som är ansvariga för informationssäkerhet och personuppgiftshantering ambitiöst med integritetsfrågor samt dataskydd, och man uppvisar en stor förståelse samt en god kunskap för dataskyddsförordningen och dess krav. I dagsläget finns det en tydlig ansvarsfördelning kring dataskyddsarbetet inom kommunen, och man påvisar även ambitioner att fortsätta utveckla verksamhetens dataskyddsorganisation för att skapa en förbättrad samordning av arbetet med personuppgifter.

Den viktigaste förbättringspunkten som EY rekommenderar 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 också att kommunen jobbar vidare inom området utbildning och medvetenhet, samt med rutinerna för att genomföra konsekvensbedömningar på befintliga personuppgiftsbehandlingar.

Stockholm den 28 maj 2021

Helena Törnqvist, Partner, EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4. Bilaga 1: Förteckning över intervjuade funktioner

4.1. Södertälje kommun

- Informationssäkerhetsansvarig
- Kommungemensam DSO
- Dataskyddssamordnare för kommunens kontor

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5. Bilaga 2: Dokumentförteckning

5.1. Södertälje kommun

- Informationssäkerhetspolicy_Dnr20-254_20201028
- Riktlinjer för hantering av personuppgifter
- Roller och gränsdragningar i GDPR-organisationen 2021
- Södertalje-riktlinjer-informationssäkerhet
- GDPR Södertälje Slutrapport v.2
- GDPR information på intranätet Kanalen
- GDPR introduktion till personuppgiftsansvarig
- Information till registrerade inom försörjningsstöd (SK)
- instruktion_pubavtal_1_0
- Kommunstyrelsen-dokumenthanteringsplan-2020
- mall_underbitraden_1_0
- Medborgarnas rättigheter
- Personuppgiftsbehandling i tredje land - Dataskyddsförordningen (GDPR) - Södertälje kommuns intranät
- Personuppgiftsbiträdesavtal Telge - Ta fram avtal
- Personuppgiftsincidenter och andra överträdelser_v1.0
- Presentation Utbildningsplan - verksamhetsspecifik utbildning
- Process PU-incidenter
- Process utlämning-borttag-flytt av personuppgifter GDPR
- pub-avtal revision 2020-01-02_slutlig
- Registerförfrågning rutin per kontor
- Rutin för incidenthantering
- samtycke-fran-avbildad-person
- samtycke-fran-avbildad-person---barn
- Säkra meddelanden – användarinstruktion
- Tröskelanalys för konsekvensbedömning - v1.01
- UTKAST-Checklista-personuppgiftsincident
- Vägledning för riskhantering
- Vägledning privacy by design and default

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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 (DSO): 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 Integritetsskyddsmyndigheten.

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.

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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.

Profilering: 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 Integritetsskyddsmyndigheten 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 personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.