Kommunrevisorerna granskar

Efterlevnad av dataskyddsförordningen GDPR

2020-10-20

Angående granskningen

Revisionsuppdraget är ett kommunalt förtroendeuppdrag och revisorerna är direkt ansvariga inför kommunfullmäktige och därmed indirekt inför medborgarna genom den representativa demokratin. Revisionen har uppdrag att granska de verksamheter som styrelser, nämnder och kommunala bolag bedriver.

I formell mening är varje revisor en egen myndighet, men i det praktiska revisionsarbetet sker arbetet gemensamt.

Ytterst syftar revisionen till att undersöka om verksamheten bedrivs i enlighet med uppställda mål och på ett från ekonomisk synpunkt tillfredsställande sätt.

- Revisorernas uppdrag regleras i kommunallag, aktiebolagslag, god revisionssed, ägardirektiv och reglemente.
- Revision ska utföras på ett oberoende sätt.
- Revisorerna genomför grundläggande granskning, granskning av delårsrapport och årsredovisning och fördjupade granskningar.

Revisorerna ska därför objektivt, opartiskt och sakligt, självständigt granska den verksamhet som styrelse, nämnder och beredningar bedriver. Revisorerna ska också bedöma om de förtroendevalda ledamöterna i nämnder och styrelser har tillräcklig styrning och kontroll över verksamhetens ekonomi, prestationer och kvalitet.

Revisorernas uttalanden och bedömningar finns i revisionsberättelser och granskningsrapporter. En ambition i revisorernas arbete är att deras rekommendationer i samband med granskning ska kunna användas av verksamheterna för att åstadkomma effekter i deras förbättringsprocess.

Kontaktuppgifter

Om kommunrevisorernas uppdrag

kommunrevisionen@umea.se

Om innehållet i denna granskning

Michael Luxemburg, konsult

michael.luxemburg@se.ey.com

Ordförande i kommunrevisionen

Ewa Miller, ordförande
ewa.miller@umea.se

Umeå kommun

Granskning av efterlevnad av Dataskyddsförordningen GDPR

Oktober 2020

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

Sammanfattning

EY har på uppdrag av Umeå 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, d.v.s. kommunstyrelsen och övriga nämnder, 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 kommunen.

Granskningen genomfördes med utgångspunkt i kommunens centrala arbete med personuppgiftssäkerhet. Då varje nämnd är personuppgiftsansvarig och är ansvarig för behandlingen av personuppgifter i sin verksamhet beslutades även att följande nämnder skulle granskas närmare, genom separata intervjuer med personuppgiftskoordinatorer och genomgång av dokumentation för vardera nämnd: Kommunstyrelsen (KS), Gymnasie- och vuxenutbildningsnämnden (GVN), Individ- och familjenämnden (IFN) samt Fritidsnämnden (FN).

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 augusti 2020. Enligt metoden bedöms verksamhetens mognadsgrad enligt 116 punkter på en skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Den genomsnittliga mognadsgraden är baserat på snittet av mognadsgraden för de respektive 12 områdena.

Baserat på den analys och granskning som genomförts bedöms Umeå kommun ha den genomsnittliga mognadsgraden 2,4 av 5,0. 2,4 är en förhållandevis låg nivå jämfört med vad EY generellt observerar för kommuner, och uppfyller inte den nivå EY rekommenderar givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

Överlag bedöms mognadsgraden vara högst inom incidenthantering och information till registrerade. Det finns tydlig och omfattande information till registrerade och tydliga kontaktvägar till kommunen via hemsidan, och de undersökta förvaltningarna jobbar aktivt med information. Incidenthantering är det enda område för personuppgiftssäkerhet specifikt där det finns tydliga riktlinjer. Incidenthanteringsprocessen kan bedömas fungera i praktiken i förvaltningarna, även om det återstår arbete med att dokumentera rutiner.

Umeå kommuns arbete med personuppgiftshantering har flera förbättringsområden. Det saknas beslutade riktlinjer och rutiner inom ett flertal områden och det återstår mycket operativt arbete för att uppnå en ändamålsenlig nivå. EY rekommenderar att styrningen utvecklas framför allt inom

- Organisation och ansvar, där resursfördelning och arbetsinstruktioner bör styra arbetet med utformning och dokumentation av övergripande riktlinjer och rutiner mot att samordnas centralt i högre utsträckning, resurser bör tilldelas för operativt arbete i

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

förvaltningarna och informationssäkerhetssamordnarens placering i organisationen bör ses över;
- Kontroll, där man följer upp arbetet regelbundet för att säkerställa att verksamheten lever upp till de krav som lagen, kommunen och dess invånare förväntar sig;
- Utbildning, där man bör säkerställa att alla medarbetare tar del av regelbundna utbildningar.

Dessa punkter skulle kunna åtgärdas med hjälp av att kommunen implementerar ett ledningssystem för informationssäkerhet (LIS). LIS är ett stöd för att styra informationssäkerhetsarbetet och innebär att man jobbar strukturerat och systematiskt med ledningens uttalade stöd. Införande av detta skulle hjälpa kommunen att arbeta mer effektivt och minska den resursbrist som i dagsläget noteras i förvaltningarna. I förlängningen kan man på så sätt uppnå en fullt ändamålsenlig modell för arbetet med GDPR.

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

Innehållsförteckning

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

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 uppdagats.
- 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 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. Datainspektionen har också inlett andra inspektioner inom ramen för dataskyddsförordningens efterlevnad.

Då Umeå 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 Umeå kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur man uppfyller de krav som förordningen stipulerar.

Granskningen ska svara på följande tre revisionsfrågor:

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

- Arbetar Umeå kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Umeå kommun policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Umeå 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 utgår från arbetet som kommunen bedriver på central nivå men inkluderar även arbetet som bedrivs inom följande utvalda nämnder: Kommunstyrelsen (KS), Gymnasie- och vuxenutbildningsnämnden (GVN), Individ- och familjenämnden (IFN) samt Fritidsnämnden (FN). 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 den centrala dataskyddsorganisationen och de utvalda nämnderna 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

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. 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 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.

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

- Maj-augusti 2020 – Dokumentanalys, utförande av arbetsmöten (2020-05-25, 2020-06-09, 2020-06-10, 2020-06-11, 2020-06-11), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport, samt faktagranskning av intervjuade nyckelpersoner.
- September 2020 – Kvalitetssäkring av EY:s verksamhetsrevisorer och slutgiltig presentation för kommunens förtroendevalda revisorer.

1.5. Definitioner

Se bilaga 3.

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 konstateras att Umeå kommun och dess verksamheter har en lägre mognadsgrad inom arbetet för att säkerställa ändamålsenlig hantering av personuppgifter, jämfört med vad som kan förväntas av en offentlig verksamhet av motsvarande storlek och karaktär.

Från centralt håll har ett i flera hänseenden ambitiöst arbete skett. Övergripande styrdokumentation är i vissa hänseenden väl utvecklad och kompetensen samt ambitionen att stötta i nämndernas arbete är god. Organisationen är också tydligt utformad. Däremot noteras det att informationssäkerhetssamordnaren (ISS) inte innehar en central befattning utan är placerad under tekniska nämnden, samt att mycket ansvar är fördelat ut till nämnderna vars förvaltningar och ansvariga roller inte alltid har erhållit tillräckligt stöd för att utföra ändamålsenligt arbete. Dessutom har en betydande andel anställda inte genomgått relevanta utbildningar vilket medför risk att de behandlar personuppgifter felaktigt. Det är också noterbart att kommunen har överlämnat ansvaret för utformning av rutiner till nämnderna i högre grad än vad EY generellt observerar för kommuner.

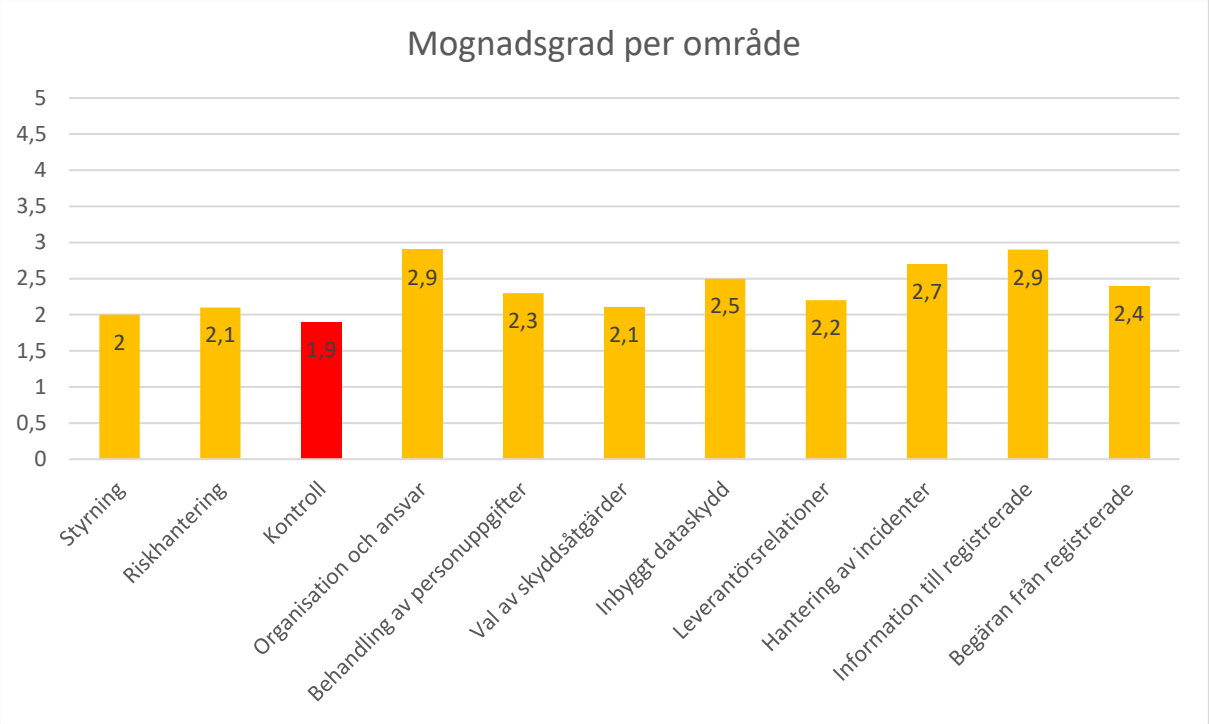
De granskade nämnderna, d.v.s. Kommunstyrelsen (KS), Gymnasie- och vuxenutbildningsnämnden (GVN), Individ- och familjenämnden (IFN) samt Fritidsnämnden (FN), saknar beslutade riktlinjer och rutiner inom alla områden förutom incidenthantering. I praktiken har nämndernas förvaltningar i sitt arbete istället till största del förlitat sig på stöttning från DSO och ISS, vars arbetsuppgifter därmed har ökat i omfattning. DSO och ISS har med tiden bidragit med fler dokumenterade rutiner som förvaltningarna kan arbeta utefter. Utöver avsaknad av rutiner har det varit svårt att nå ut med relevant information till medarbetare inom förvaltningarna, vilket bidrar till en ökad arbetsbörda för personuppgiftskoordinatorerna som därmed behöver arbeta mer operationellt med frågor kring hantering av personuppgifter, snarare än att vara koordinerande och stötta verksamheten vid behov. I dagsläget har de granskade nämndernas förvaltningar, med undantag av FN:s förvaltning, mycket återstående arbete och hindras av betydande resursbrist. De flesta personuppgiftskoordinatorer har tilldelats sina roller utöver befintliga heltidstjänster vilket har gjort det svårt att utföra den stora mängd initiala arbete som krävs för att hantera de frågor som dataskyddsförordningen stipulerar. EY:s analys tyder på att resursbristen kan avhjälpas genom att kommunen från centralt håll utformar fler riktlinjer och mallar eller rutiner som nämnderna kan ta del av, samt att utbildningsinsatser sker i högre omfattning så att arbetet kan ske mer proaktivt istället för reaktivt. Ytterligare noterbart är att kontroll av arbetet till stor del saknas. En brist på kontrollrutiner från centralt håll medför att förvaltningarna inte vet vad som bör prioriteras och riskerar att inte leva upp till kommunens förväntningar. För FN, som är ansvarig för klart minst mängd personuppgifter, skiljer sig iakttagelserna något eftersom de har kommit betydligt längre i sitt arbete i förhållande till mängden personuppgifter.

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

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 1: Mognadsgrad per område

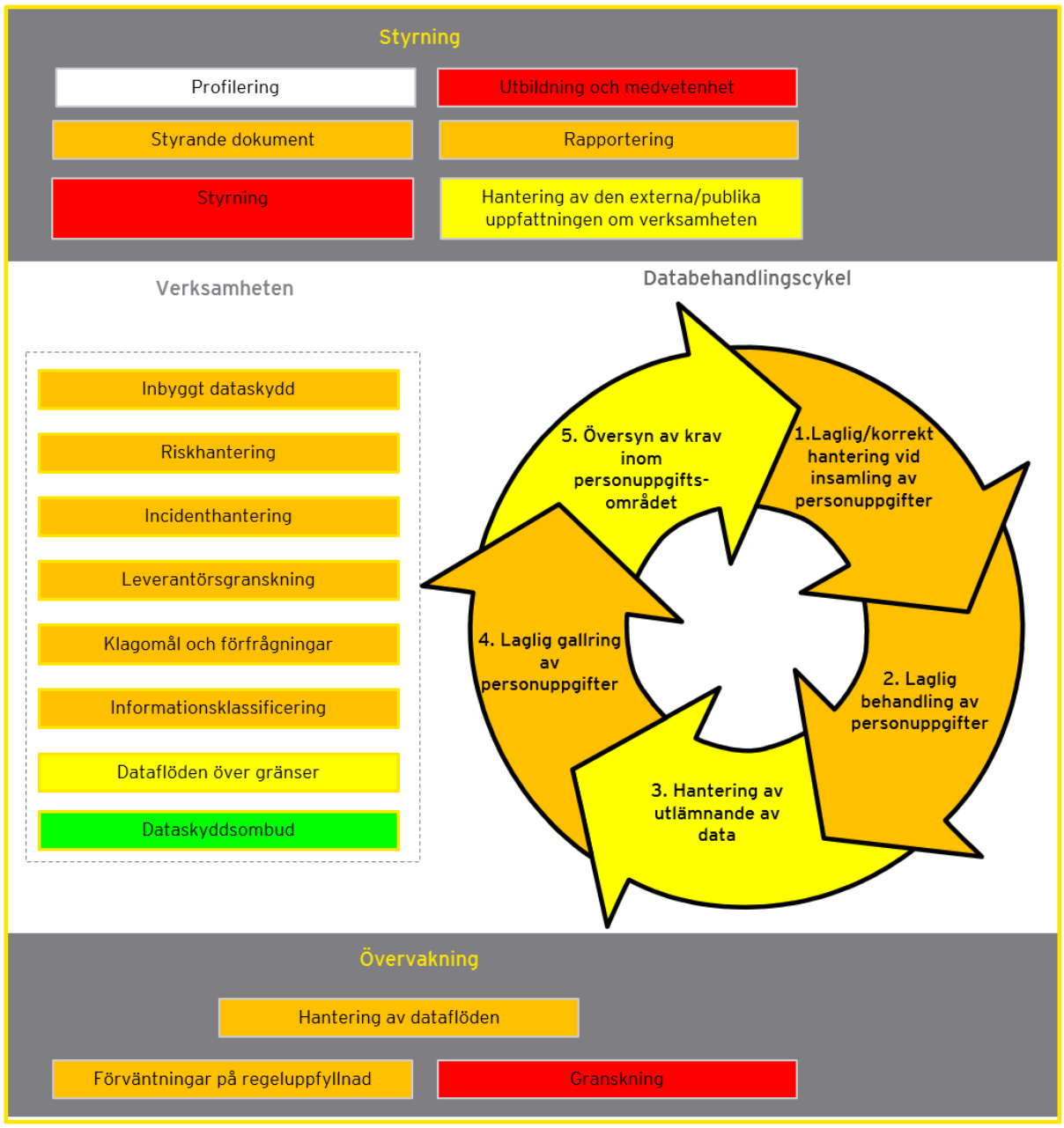


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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: 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.

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	Umeå kommun har en övergripande informationssäkerhetspolicy antagen av kommunfullmäktige. Den är senast reviderad 2013. Det finns en övergripande konkretisering av informationssäkerhetspolicyn för kommunens verksamheter. Strukturen på dokumentationen är tydlig. Nämnderna saknar dokumenterade och beslutade rutiner för hur informations-säkerhet och personuppgiftshantering omsätts i praktiken. Detta gäller samtliga områden med undantag för incidenthantering. GVN har riktlinjer för hantering av personuppgifter i molntjänster, som täcker in flera aspekter av arbetet med personuppgiftssäkerhet. Det saknas rutiner för att följa upp om regelverk följs. DSO har delat ut en ”att göra-lista” till förvaltningarna, men brister och förbättringsområden har inte analyserats formellt eller dokumenterats. Åtgärdsplaner saknas. Ansvaret för att arbetet med personuppgiftssäkerhet lever upp till lagkraven har fördelats ut till nämnderna. Det är upp till ledningen för varje förvaltning att avgöra prioriteringar och hur arbetet ska ske i praktiken. Förvaltningarna saknar tydliga riktlinjer eller krav från ledningen, både från centralt håll och i respektive förvaltning. Personuppgiftskoordinatorerna förlitar sig istället på instruktioner från och dialog med DSO och ISS. Varje nämnd ansvarar för sina egna insamlade personuppgifter. Det finns en instruktion i RegIT för hur biträdande nämnd bör hantera personuppgiftsansvarig nämnds personuppgifter. Det framgår också i kommunens reglemente att den personuppgiftsansvarige nämnden	Det finns övergripande instruktioner inom flera områden men endast ett fåtal rutiner på en mer detaljerad nivå har dokumenterats och beslutats av nämnderna. Dokumenterade rutiner saknas exempelvis för granskning, rapportering, uppdatering av registerförteckning, gallring av personuppgifter samt hantering av begäran från registrerade. Det saknas rutiner för att följa upp om regelverk följs och det saknas åtgärdsplaner. Förvaltningarna saknar tydliga instruktioner och prioritetsordningar för att hantera de utestående riskerna. Respektive nämnd har tilldelats ansvar att besluta och prioritera arbetet kring personuppgiftssäkerhet, men tydliga prioriteringar och instruktioner kring detta har inte beslutats och kommunicerats i större omfattning. Ingen uppföljning har gjorts av hur behandlingen av personuppgifter går till i praktiken när en nämnd behandlar personuppgifter som en annan nämnd är ansvarig för.	2,0

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

	ansvarar för att lämna instruktioner till biträdande nämnd.		
Riskhantering	Riskanalyser har tidigare utförts för IT-system inom ramen för kommunens informationssäkerhetsarbete. SKR:s verktyg KLASSA har använts för riskanalyser för flertalet system och införande av nya system, men ingen regelbunden riskanalys eller uppdatering genomförs. I kommunens IT-upphandlingsmodell framgår det att riskanalys, och vid behov konsekvensbedömning, ska genomföras innan upphandling. DSO har tagit fram en kort instruktion och mall för konsekvensbedömning som uppdaterats löpande efter feedback från koordinatorer. Mycket arbete återstår i förvaltningarna.	Riskanalys har inte skett för samtliga system eller verksamheter där det är nödvändigt, och det finns ingen plan för uppdatering av gamla riskanalyser. Flertalet konsekvensbedömningar återstår att genomföra.	2,1

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

Kontroll	DSO är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Samtliga granskade förvaltningar rapporterar regelbundet incidenter till nämnderna. Förvaltningarnas personuppgifts-koordinatorer har frekvent kontakt med DSO för rådgivning och vägledning. DSO har tagit fram en ”att göra-lista” som förvaltningarna utgår från i sitt arbete. ISS beskriver i en årsberättelse övergripande status för arbetet med informationssäkerhet. Det sker ingen formaliserad rapportering till nämnd eller förvaltningsledning, exempelvis genom rapporter som ger en noggrannare bild av status på arbetet och granskning av efterlevnad inklusive åtgärdsplaner. Förvaltningarna uppger varierande intresse från ledning och nämnder. Fritidsförvaltningen uppger ett engagemang från förvaltningschef och har på egen hand skapat ett visst intresse hos nämnden. Övriga förvaltningar uppger att deras arbete till stor del förbises. Det finns inte dokumenterade rapporteringskrav till kommunledningen eller fastslagen kontrollplan för verksamheterna. DSO rapporterar dock på eget initiativ till stadsledningen vid behov, men minst en gång per år.	Det finns ingen granskningsplan eller internkontrollfunktion med fokus på att dataskyddsarbetet är i enlighet med dataskyddsförordningens krav. Det bör finnas dokumenterad granskning av efterlevnad med åtgärdsplaner för varje nämnd, som uppdateras exempelvis årligen. Det finns inga dokumenterade krav för när rapportering till ledning bör ske.	1,9

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	Dataskyddsorganisationen är tydligt utformad och dokumenterad. Både den centrala dataskyddsorganisationen och personuppgiftskoordinatorerna innehar lämplig kompetens. DSO och ISS har heltidstjänster. Noterbart är att ISS är placerad i förvaltningen för Teknik och fastighet under Tekniska nämnden, även om hon i den rollen har ett ansvar att stödja förvaltningarna för samtliga nämnder i arbetet med informationssäkerhet, samt bör rapportera till kommunledningen centralt. Umeå kommun är en av Sveriges största kommuner, både sett till antal anställda och antal invånare. Kommunen bedriver dessutom mycket arbete med digitalisering, där dataskydd och informationssäkerhet spelar en viktig roll i utvecklingen. ISS och DSO ska stötta samtliga nämnder i arbetet med GDPR i denna kontext. Den stora majoriteten av de intervjuade personuppgiftskoordinatorerna har fått sina roller tillagda utöver befintliga heltidstjänster. Ingen prioritetsordning har angivits, vare sig för uppdelningen mellan heltidstjänst och koordinatorrollen eller inom ansvarsområdena som koordinatorrollen innebär. Förvaltningarna upplever att tiden inte alltid räcker till för att hinna med alla arbetsuppgifter som rollen som personuppgiftskoordinator i sin nuvarande utformning kräver. Förvaltningarna upplever även ett stundtals lågt intresse för dataskyddsfrågor från förvaltningsledningarna. Förvaltningarna har ingen fastslagen dokumentation kring dataskyddsorganisation eller ansvarsfördelning.	Resurserna för dataskyddsarbetet på central nivå kan anses vara förhållandevis små relaterat till storleken på kommunen. Resurser för operativt informationssäkerhets-arbete i förvaltningarna saknas. Detta påverkar förvaltningarnas mognadsgrad samt digitaliseringsarbetet. Personuppgiftskoordinatorerna saknar i vissa hänseenden stöd och förutsättningar för att kunna utföra de uppgifter de är ålagda att göra. Detta innefattar tid, dokumenterade rutiner, tydliga handlingsplaner samt medvetenhet bland anställda för att bli mer självgående och därmed avlasta koordinatorerna i det dagliga arbetet.	2,6

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

Behandling av person-uppgifter	Umeå kommun använder sig av inventariesystemet RegIT som registerförteckning för att hantera personuppgifter. Detta har använts sedan flera år för att uppfylla kraven i PUL. Från både centralt håll och förvaltningarna har det noterats att registerförteckningen inte är uppdaterad, och att det i vissa fall återstår mycket arbete. Uppdatering av registerförteckning görs oftast på initiativ och med stöd av personuppgiftskoordinatorerna, vilket de inte har tid att göra för varje behandling eller system. Personuppgifter utanför system är inte heller uppdaterade. Gallring ska ske enligt dokumenthanteringsplaner, men det är inte klarlagt huruvida detta sker och ansvaret inom förvaltningarna är inte tydligt. Därtill saknar man rutiner för att säkerställa att personuppgifter endast behandlas för de ändamål de samlades in för.	Registerförteckningen är inte komplett eller fullt uppdaterad för samtliga behandlingar. Det saknas rutiner eller kontroller för att säkerställa registerförteckningens fullständighet och riktighet över tid. 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.	2,3

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	Det finns en övergripande riktlinje för informationsklassificering. Klassificering av information sker med KLASSA. ISS är ofta med i processen. Förvaltningarna har kommit olika långt i detta arbete. För koordinatorerna i KS och IFN råder det oklarhet kring vems ansvaret är. GVN vet att klassning har skett 2018-2019, men inte ifall uppdatering sker. FN bedömer att de ligger i fas med klassningarna. Avseende utbildning har de centralt ansvariga inom dataskydd 15 minuter för en kommunövergripande introduktion för nyanställda. Det finns även en dataskyddsdag som organiseras en dag per år där anställda kan delta frivilligt. De är fullbelagda. Intranätet är tydligt och utförligt, men det har noterats att det är svårt att nå ut till alla 12 500 anställda, särskilt de som inte har dator. På intranätet finns även en powerpointpresentation med grundläggande information för chefer att använda exempelvis vid arbetsplatsträffar. Det har även tagits fram ett koncept med nano-utbildningar (löpande korta webb-utbildningar) för informationssäkerhet. Det bedöms att cirka 30% av medarbetarna med mailadresser har genomgått denna. En nano-utbildning för GDPR har varit påtänkt. Det finns inget krav på att gå igenom någon utbildning utöver introduktionen. DSO har en 3 timmars baskurs för koordinatorer. Det finns även 10 lektioner online för koordinatorerna att utföra när de vill. Samtliga koordinatorer, ISS och DSO träffas en gång i månaden för att diskutera frågor och utbyta erfarenheter. ISS och DSO har stående informationspunkter och DSO har under träffarna också hållit kortare utbildningar i frågor som koordinatorerna bedömt viktiga att få mer kunskap om.	Rutiner som säkerställer att samtlig information blir klassificerad har inte implementerats. Kommunen genomför inte regelbundna utbildningar med alla relevanta anställda. Det finns vidare ingen rutin för att säkerställa att alla anställda tar del av de utbildningar som erbjuds.	2,2

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

Inbyggt dataskydd	KLASSA-ramverket används vid nyanskaffning för att bedöma att kommunens databehandling uppfyller kraven för personuppgifter, vilket även resulterar i viss lagrings- och uppgiftsminimering vid ny upphandling. Lagring- och uppgiftsminimering för befintliga system sker inte enligt fastställda rutiner. Kommunen har många gamla IT-system som inte har stöd för exempelvis tvåfaktorsautentisering eller önskvärda behörighetsstrukturer.	Flera av kommunens IT-system stödjer inte moderna krav på dataskydd.	2,5
Hantering av leverantörs-relationer	Kommunen använder sig av en lätt modifierad version av SKR:s mall för PUB-avtal. DSO bedömer att kommunen som helhet har PUB-avtal med hälften av leverantörerna där det är behövligt. Samtliga förvaltningar jobbar aktivt med att upprätta PUB-avtal för leverantörer som behandlar personuppgifter åt kommunen. Det finns ingen rutin för att regelbundet genomlysa avtal och uppdatera dessa vid behov, eller för att kontrollera att leverantören efterlever avtalat ansvar avseende behandling av personuppgifter. Kommunen använder vissa system som har datalagring utanför EU/EES. Vanligaste scenariot är att en underleverantör är exempelvis Google eller Amazon. Det finns PUB-avtal med både Google (skolan) och Microsoft (IT) som båda har tecknade Standard Contractual Clauses (SCC) med personuppgiftsansvariga. Som myndighet drabbas personuppgiftsansvarig också av problematiken kring molntjänster och utländsk lagstiftning som t.ex. CLOUD Act. Därför är kommunens PUB-mall modifierad att fånga upp var underbiträden har sina säten.	PUB-avtal har ännu inte upprättats med många relevanta leverantörer. Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.	2,3

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 incidenter	Nämnderna har antagit riktlinjer för incidentrapportering. De är baserade på den övergripande riktlinje som tagits fram centralt. IFN och GVN har även tillhörande rutiner, som DSO dock sedan tidigare inte bedömt varit tillämpbara och rekommenderat att de justeras. Varje personuppgiftsansvarig ska upptäcka, utreda, åtgärda och anmäla incidenter. Utöver nämnda utbildningsinsatser i området *Val av skyddsåtgärder* har det genomförts begränsat med utbildningsinsatser kring incidenthantering. FN har genomfört en utbildning med alla chefer där rapportering av incidenter ingick och cheferna där har fått i uppdrag att utbilda sin personal. DSO brukar trycka på vikten av att rapportera incidenter i samband med de 7,5 minuter som han har under utbildningen för nyanställda. Det har noterats att antalet incidenter skiljer sig väsentligt mellan olika förvaltningar, vilket skulle kunna bero på att många incidenter passerar utan att rapporteras. Det finns inga etablerade rutiner på plats som kontrollerar att de interna instruktionerna eller rutinerna gällande personuppgiftsincidenter efterlevs.	Rutiner för incidenthantering finns inte dokumenterade i samtliga förvaltningar. Det saknas en rutin för att granska efterlevnaden av rutinerna gällande personuppgiftsincidenter, i de fall rutiner finns på plats.	2,6
Information till registrerade	Vid insamling av personuppgifter lämnas information till den registrerade om hur personuppgifterna kommer användas. Det finns mallar på intranätet som varje förvaltning kan ta del av. Samtycke undviks i största möjliga mån i kommunen. DSO har varit involverad för att ta fram blanketter och hantera frågan om laglig grund. GVN använder samtycke i viss utsträckning. Dessa loggas digitalt och är enkla att återkalla för de registrerade.		2,9

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

Begäran från registrerade	Det finns en kontaktväg via mail och telefon där registrerade kan framföra förfrågningar och klagomål. Det finns utförlig information på hemsidan för de registrerade. Det finns en kommunövergripande rutin som tagits fram av DSO och som är beslutat av stadsdirektören. DSO har tagit fram mallar som personuppgiftsansvarig kan utgå från för att uppfylla de olika kraven gällande rätten till information. Mallarna och ytterligare information om rättigheterna finns tillgängliga på intranätet. Förvaltningarna saknar dock dokumenterade rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. Kommunövergripande rutiner gällande dessa frågor planeras att införas under hösten. Det har observerats att rutinen för registerutdrag är inte är välkänd bland verksamheterna samt att verksamheterna kan blanda ihop begäran om allmän handling och registerutdrag, vilket kan resultera i att den registrerades rättigheter inte tillgodoses.	Det saknas dokumenterade rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. Rutinen för registerutdrag är inte välkänd bland verksamheterna.	2,4
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 flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera sex övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom förvaltningens dataskydd och informationssäkerhetsarbete.

Styrning

Det finns övergripande riktlinjer för arbetet med personuppgiftshantering från centralt håll, men tydlig styrning av det praktiska arbetet saknas till stor del. Förvaltningarnas arbete är inte tydligt kravställt från nämnder eller kommunledning, och som konsekvens har arbetet i respektive förvaltning försvårats. I praktiken har personuppgiftskoordinatorerna, med stöd från DSO och ISS, blivit ålagda att utföra respektive förvaltnings arbete, utöver att ha sina koordinerande roller. Arbetet med att komma ikapp med de analyser och dokumentation av relevanta behandlingar och system som erfordras enligt dataskyddsförordningen är stort, och kräver ett strukturerat stöd genom hela organisationen. Dokumenterade och beslutade rutiner för personuppgiftsbehandlingsprocesser och granskning av efterlevnad av dessa saknas också till stor del. För att åtgärda dessa problem rekommenderar EY att Umeå kommun utvecklar styrningen framför allt inom

- Organisation och ansvar, där resursfördelning och riktlinjer bör styra arbetet mot att samordnas centralt i högre utsträckning, resurser bör tilldelas för operativt arbete i förvaltningarna och ISS placering i organisationen bör ses över;
- Kontroll, där man följer upp arbetet regelbundet för att säkerställa att verksamheten lever upp till de krav som lagen, kommunen och dess invånare förväntar sig;
- Utbildning, där man bör säkerställa att alla medarbetare tar del av regelbundna utbildningar.

Genom att åtgärda dessa punkter kan kommunen arbeta mer effektivt och mitigera den resursbrist som i dagsläget noteras i förvaltningarna. EY noterar att ett ledningssystem för informationssäkerhet (LIS) skulle kunna implementeras för att åtgärda dessa områden. Områdena beskrivs i närmare detalj nedan. En mer utvecklad struktur och styrning inom arbetet med personuppgifter skulle också kunna samverka med digitaliseringsarbetet. Personuppgiftskoordinatorerna kan med fördel inneha arbetsuppgifter inom IT och digitalisering, då utveckling av verksamheten utifrån digitalisering är beroende av ett väl fungerande informationssäkerhetsarbete.

Organisation och ansvar

Umeå kommun har fördelat ut ansvaret till respektive nämnd eftersom respektive nämnd juridiskt är personuppgiftsansvarig. Detta innebär dock inte att hela arbetet med personuppgiftssäkerhet behöver ske decentraliserat. DSO har sedan införandet av GDPR utvecklat fler mallar och instruktioner med tiden. Även om detaljerna i varje förvaltnings arbete kan skilja sig åt, rekommenderas kommunen att i högre grad fortsätta arbetet som DSO påbörjat med att utforma riktlinjer och rutiner centralt för varje nämnd att fastslå och anpassa vid behov. Detta har potential att accelerera arbetet och göra det mer

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

resurseffektivt, då riktlinjer och rutiner kan utformas av en gemensam arbetsgrupp istället för separat i varje förvaltning. Därtill bör det tilldelas resurser för operativt arbete i förvaltningarna, då detta i dagsläget saknas.

Informationssäkerhetssamordnarens placering i organisationen bör ses över. Placeringen under Tekniska nämnden medför att övriga förvaltningars medarbetare riskerar att få intrycket att ISS enbart hanterar IT-frågor, samt ger ISS mindre mandat att säkerställa att ändamålsenligt arbete sker inom varje förvaltning. Detta kan bidra till att förvaltningarna inte inser att det är deras respektive ansvar att arbeta ändamålsenligt med personuppgiftshantering, utan ser det som en IT-fråga där ansvaret ligger någon annanstans. En placering ute i en specifik förvaltning tyder också på att informationssäkerhetsarbetet är nedprioriterat och gör rapporteringsvägen till ledningen längre. Dessutom är det vanligt att ansvar för IT respektive informationssäkerhet är separerat, då Tekniska nämndens ansvar i regel är att upprätthålla IT-tjänster som kostnadseffektivt möter verksamhetens behov vilket kan stöta sig mot säkerhetsmässiga överväganden. I det hänseendet brukar det vara lämpligt att ansvarig för informationssäkerhet inte rapporterar till IT-chef. Den gemensamma grunden för dessa argument är att informationssäkerhet är en kommunövergripande och viktig fråga, och ISS placering i organisationen bör avspegla detta.

Kontroll

EY rekommenderar att kommunen utformar rutiner för regelbundna granskningar för att tydligare identifiera riskområden och potentiella brister samt bestämma prioritetsordning och tidsplan för nödvändiga åtgärder. Genom dessa kan man säkerställa att verksamhetens rutiner lever upp till lagkrav och interna riktlinjer. Kommunen rekommenderas även att fastställa ett rapporteringskrav gällande frekvens och innehåll för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen. EY rekommenderar vidare att DSO eller övrig kontrollfunktion genomför formella periodiska granskningar med tillhörande åtgärdslistor och planer, inkluderande tidsplaner, för förvaltningarna att agera utefter.

Utbildning och medvetenhet

Utbildning- och informationsinsatser för att öka kunskapsnivån och medvetenheten genomförs, men det har konstaterats att det är en utmaning att nå ut till samtliga medarbetare. En kort introduktion kring informationssäkerhet genomförs med nyanställda. Därtill skickas en nano-utbildning inom informationssäkerhet till alla medarbetare med mailadresser en gång per år. Nano-utbildningarna är inte obligatoriska och vid uppföljning har det konstaterats en generellt låg genomförandegrad. Det finns inte heller någon motsvarande utbildning för GDPR specifikt. Flera personuppgiftskoordinatorer har noterat att medvetenheten bland medarbetarna är låg. Detta försvårar arbetet för de ansvariga. Dessutom kan instruktioner såsom förvaltningarnas incidenthanteringsdokument kunna vara verkningslösa om inte personalen är medveten om att instruktionerna existerar eller när de är tillämpliga. Kommunen bör därför se till att alla relevanta medarbetare genomför utbildningar

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

regelbundet, exempelvis en gång per år, där GDPR täcks in specifikt. För de mest kritiska verksamheterna – skolan och vården – bör dessa utbildningar vara särskilt anpassade och kontakten tätare mellan förvaltningarnas ansvariga och verksamheternas medarbetare. Utbildningarna bör uppdateras alltjämt som lagkraven blir tydligare och nya exempel finns tillgängliga.

Inbyggt dataskydd

Flera av kommunens IT-system stödjer inte moderna krav på dataskydd rörande exempelvis tvåfaktorsautentisering eller behörighetsstrukturer. Detta leder till att systemstöd inte alltid är designade för att optimera hantering av personuppgifter samt i förlängningen en risk för bristande laguppfyllnad. Umeå kommun bör accelerera arbetet med moderniseringen av IT-systemen. EY rekommenderar att kommunen inför ett tydligare strategiskt fokus på digitalisering och informationssäkerhet och genom tydliga direktiv prioriterar kommunens digitala modernisering.

Leverantörsrelationer

EY rekommenderar att Umeå kommun slutför inventeringen av de IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer, samt ingår PUB-avtal med samtliga leverantörer där det är relevant.

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. Revisionsfrågor

Revisionsfrågorna besvaras utifrån granskningen som helhet i en sammanvägd bedömning av resultatet av granskningarna på förvaltningsnivå och central nivå. I den sammanlagda bilden har skillnaderna förvaltningarna emellan inte ansetts påverka den totala bedömningen då det övergripande och slutgiltiga ansvaret för efterlevnad av dataskyddsförordningen ligger på kommunstyrelsen.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Arbetar Umeå kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?	Umeå kommun bedöms inte uppfylla de krav och regleringar som införts i och med dataskyddsförordningen (GDPR). Svaret grundar sig främst på bristerna i centralt initiativ och styrning gentemot förvaltningarna.	
Är Umeå kommuns policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?	Umeå kommuns riktlinjer och instruktioner på personuppgiftsområdet bedöms som icke ändamålsenliga med avseende på dataskyddsförordningen (GDPR). Informationssäkerhetspolicyn och övergripande riktlinje för verksamhet bedöms som ändamålsenliga, men flera riktlinjer och rutiner som bör finnas på plats i förvaltningarna saknas.	
Har Umeå kommun ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?	Umeå kommun bedöms inte ha en ändamålsenlig kontroll och uppföljning med avseende på dataskyddsförordningen (GDPR). Umeå kommun genomför begränsad kontroll och uppföljning på kommunövergripande nivå och det saknas en strukturerad granskningsplan. Ej heller finns dokumenterade rutiner för uppföljning på verksamhetsnivå och således sker ingen rapportering kring uppföljning och efterlevnad. Den samlade bilden är att resurser saknas för att detta ska gå att genomföra.	

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. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av huruvida arbetet kring personuppgiftshantering i Umeå 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.

Umeå kommun uppnår mognadsgraden 2,4 av 5,0. Detta är en förhållandevis låg nivå jämfört med vad EY generellt observerar för kommuner, och uppfyller inte den nivå EY rekommenderar givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

Överlag bedöms mognadsgraden vara högst inom information till registrerade och incidenthantering. Det finns tydlig och omfattande information till registrerade och tydliga kontaktvägar till kommunen via hemsidan, och de undersökta förvaltningarna jobbar aktivt med information. Incidenthantering är det enda område för personuppgiftssäkerhet specifikt där det finns tydliga riktlinjer fastslagna nämnderna och processen kan bedömas fungera i praktiken i förvaltningarna, men det återstår arbete med att dokumentera rutiner.

Den viktigaste övergripande förbättringspunkten rör styrning. EY rekommenderar att Umeå kommun prioriterar att förbättra följande tre områden, där en tydligare styrning lägger grunden för att framsteg ska ske:

- Organisation och ansvar. Ansvaret för arbetet med personuppgiftssäkerhet har i hög utsträckning fördelats ut till respektive juridiskt ansvariga nämnd. Varje nämnds förvaltning har i sin tur utsett personuppgiftskoordinatorer men i övrigt tillsett minimal styrning för arbetet. Detta innebär att förvaltningarnas arbete är inte tydligt kravställt från varken nämnder eller kommunledning. I praktiken saknas tydligt ansvar och målsättningar för vem som ska utveckla riktlinjer och rutiner i förvaltningarna, och koordinatorerna har implicit fått ansvar för att både utveckla rutiner och utföra hela det praktiska arbetet, utöver att ha ett samordningsansvar. EY rekommenderar att mer ansvar för exempelvis utformning av riktlinjer och rutiner tas centralt för att underlätta och i högre grad samordna arbetet för förvaltningarna, samt att resurser tilldelas för operativt arbete i förvaltningarna, då detta i dagsläget saknas. EY rekommenderar också att informationssäkerhetssamordnarens placering i organisationen ses över, då informationssäkerhet är en kommunövergripande fråga separat från IT.
- Kontroll. Regelbundna uppföljningar av arbetet med personuppgiftssäkerhet saknas. DSO har en central roll för att granska arbetet, men det saknas fastställda rutiner för granskning och rapportering utöver incidenter. Det råder därmed oklarhet ifall kommunen lever upp till de krav som lagen och kommunens invånare förväntar sig. Utan en tydlig och fastslagen åtgärdsplan kan förvaltningarna inte heller prioritera arbetet i enlighet med vad kommunledningen förväntar sig.
- Medvetenhet. Kommunen har nått ut med utbildningsinsatser till medarbetarna i begränsad utsträckning. EY noterar att det finns ett stort behov för ytterligare utbildning inom organisationen. Utan rätt kunskaper hos medarbetarna riskerar

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

kommunen att utsättas för onödiga misstag och att de instruktioner som finns på plats inte följs. En ökad medvetenhet inom varje förvaltning underlättar också i personuppgiftskoordinatorernas arbete.

EY bedömer att dessa tre områden behöver förbättras för att Umeå kommun ska kunna uppnå ett ändamålsenligt arbete med personuppgifter och dataskydd. Detta skulle kunna hanteras genom att implementera ett ledningssystem för informationssäkerhet (LIS), som är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter. Genom att åtgärda de tre områdena, förslagsvis genom implementation av LIS, kan kommunen arbeta mer resurseffektivt och mitigera den resursbrist som i dagsläget noteras i förvaltningarna. En mer utvecklad struktur och styrning på arbetet med personuppgifter skulle också kunna samverka med digitaliseringsarbetet, för en långsiktigt hållbar plan där dataskydd inkluderas som en naturlig del i det dagliga utvecklingsarbetet.

Stockholm den 9 oktober 2020

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

5. Bilaga 1: Förteckning över intervjuade funktioner

5.1. Centrala dataskyddsorganisationen

- Dataskyddsombud
- Informationssäkerhetssamordnare

5.2. Kommunstyrelsen

- Fyra personuppgiftskoordinatorer

5.3. Individ- och familjenämnden

- Tre personuppgiftskoordinatorer

5.4. Gymnasie- och vuxenutbildningsnämnden

- Tre personuppgiftskoordinatorer

5.5. Fritidsnämnden

- Två personuppgiftskoordinatorer

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 2: Dokumentförteckning

6.1. Centrala dataskyddsorganisationen

- Att lämna ut en allmän handling och att vägra
- E-post regler
- Filter och loggning av internettrafik
- Informationshantering O 362 mejl och OneDrive
- Informationssäkerhetspolicy Umeå kommun
- Instruktion för informationsklassificering
- ITU_5_Checklista
- Riktlinjer för informationssäkerhet – användare
- Riktlinjer för informationssäkerhet – verksamhet
- Rätt till information artikel 15 GDPR
- Dataskyddsorganisationen i Umeå kommun
- Inhämtning och lagring av samtyckesdokument för bilder på barn under 16 år
- Konsekvensbedömning [behandlingens namn] avseende dataskydd enligt artikel 35 dataskyddsförordningen
- Konsekvensbedömning avseende dataskydd enligt artikel 35 dataskyddsförordningen
- Modellavtal
- Reviderat reglemente för styrelse och nämnder 2020-03-30
- Samtycke för bildpublicering personer över 16 år
- Samtycke för bildpublicering, personer under 16 år
- Vad återstår att göra GDPR
- Årsberättelse informationssäkerhet

6.2. Individ- och familjenämnden

- Riktlinjer för personuppgiftsincidenthantering

6.3. Gymnasie- och vuxenutbildningsnämnden

- Bilaga Rutin hantering GDPR-incident
- Bilaga Riktlinjer personuppgifter

6.4. Fritidsnämnden

- Riktlinje Personuppgiftsincidenthantering

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

7. 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.

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

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.

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 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,

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

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