Uppsala kommun

Arbetsmarknadsförvaltningen
Tjänsteskrivelse till arbetsmarknadsnämnden

Datum:
2021-08-13

Diarienummer:
AMN-2021-00255

Handläggare:
Weronica Öhrt

Personuppgiftsrevision utifrån GDPR

Förslag till beslut

Arbetsmarknadsnämnden beslutar

1. **att** uppdra till förvaltningen att genomföra föreslagna åtgärder efter revisionens rekommendationer,

2. **att** anta revisionens förslag till tidplan för genomförande av åtgärderna.

Ärendet

Den 17 december 2020 genomförde kommunens dataskyddsombud en revision av arbetsmarknadsnämndens hantering av personuppgifter. Syftet var att säkerställa att nämnden uppfyller de krav som ställs i dataskyddsförordningen (GDPR) och föreslå eventuella åtgärder vid behov. Utifrån denna revision har förslag på åtgärder och tidplan för genomförande lämnats.

Beredning

Ärendet har beretts av kvalitetsenheten på socialförvaltningen för arbetsmarknadsförvaltningen i samarbete med dataskyddsombudet, JP infonet. Dataskyddsombudet har analyserat arbetsmarknadsförvaltningens behandling av personuppgifter gentemot dataskyddsförordningen. Revisionen analyserade nuläget av efterlevnaden av dataskyddsförordningen och identifierade förslag på åtgärder för att underlätta och förbättra arbetet med efterlevnaden av dataskyddsförordningen.

Föredragning

Dataskyddsförordningen (GDPR) ställer krav på hur personuppgifter ska hanteras för att skydda enskild personers grundläggande fri- och rättigheter och särskilt rätt till skydd av personuppgifter. Revisionen anser att arbetsmarknadsförvaltningen

har kommit en bit på vägen med implementering och att fokus framåt bör ligga på fortsatt implementering i verksamheterna och kompetensutveckling.

Revisionen rekommenderar arbetsmarknadsnämnden att vidta följande åtgärder, i prioriteringsordning[1]:

- ta fram en utbildningsplan för att öka kunskapen hos samtliga medarbetare om GDPR
- anta Artikel 30-registret som ett officiellt dokument
- fastställa vilka processer som tar vid efter att Artikel-30 registret är färdigställt
- utarbeta en rutin för att systematiskt uppdatera Artikel-30 registret
- implementera det kommungemensamma dokumentet incidentrutin i verksamheten
- implementera en rutin gällande översyn av vissa lagringsutrymmen.

Tidplanen som föreslås för genomförande av de rekommenderade åtgärderna är följande:

Augusti 2021: Anta Artikel 30-registret som ett officiellt dokument – när dokumentet är klart och godkänt av Dataskyddsombudet kommer det att informeras i nämnden. (hösten 2021)

Hösten 2021: Fastställa vilka processer som tar vid efter att Artikel 30-registret är färdigställt samt utarbeta en rutin för systematisk uppföljning av registret.

Hösten 2021: Implementera incidentrutin i verksamheten.

Hösten 2021: Ta fram en utbildningsplan för förvaltningens medarbetare.

Hösten 2021/våren 2022: Genomföra utbildningen.

Ekonomiska konsekvenser

Arbetet med implementeringen av dataskyddsförordningen är pågående i förvaltningen. Inga ekonomiska konsekvenser bör uppstå då revisionens förslag till tidsplan för genomförande av rekommenderade åtgärder delvis handlar om åtgärder som en fortsättning på arbete som redan är påbörjat. Utbildningen som föreslås tas fram centralt på kommunledningskontoret i samarbete med dataskyddsombudet.

Jämställdhetskonsekvensanalys
Då revisionen och arbetet med personuppgiftshantering handlar om samtliga personuppgifter påverkas inget kön negativt av förslaget till åtgärder och åtgärdsplanen.

Barnkonsekvensanalys
Då revisionen och arbetet med personuppgiftshantering handlar om samtliga personuppgifter påverkas barn inte negativt av förslaget till åtgärder och åtgärdsplanen.

[1] För detaljerad information identifierade risker, nuläge och åtgärder se bilaga 1, avsnitt 3 ”Åtgärdslista”

Beslutsunderlag

Tjänsteskrivelse daterad 2021-08-30

Bilaga 1: Dataskyddsombudets åtgärdsplan till Uppsala kommun Arbetsmarknadsnämnd efter genomförd personuppgiftsrevision den 17 december 2020

Bilaga 2: Förstudie av arbetet med införandet av GDPR i Uppsala kommun

Arbetsmarknadsförvaltningen

Lena Winterbom
Förvaltningsdirektör

Dataskyddsombudets åtgärdsplan till

Uppsala kommuns Arbetsmarknadsnämnd

efter genomförd personuppgiftsrevision den 17 december 2020

1. BAKGRUND

Syftet med denna åtgärdsplan är att säkerställa lagefterlevnad för Uppsala kommuns Arbetsmarknadsnämnd gällande hur personuppgifter behandlas. Dataskyddsförordningen ställer krav på hur myndigheter, företag och organisationer hanterar och behandlar personuppgifter. Som personuppgiftsansvarig nämnd måste Arbetsmarknadsnämnden ta ansvar och se till så att de personuppgifter som behandlas i nämnden behandlas på ett korrekt och lagligt sätt.

För att säkerställa att Arbetsmarknadsnämnden möter de krav som ställs upp i Dataskyddsförordningen har nämndens behandling av personuppgifter analyserats genom de lagkrav som Dataskyddsförordningen ställer upp. Analysen genomfördes för att utforska nuläget av efterlevnaden av Dataskyddsförordningen, identifiera eventuella brister och bidra till att underlätta samt förbättra det kontinuerliga arbetet med efterlevnaden av Dataskyddsförordningen. Analysen har sedan mynnat ut i denna åtgärdslista som ger nämnden ett dokumenterat nuläge på eventuella brister som återfinns i nämnden samt förslag på hur dessa brister bör åtgärdas och prioriteras.

2. METOD

Eftersom lagefterlevnad är ett omfattande arbete i nämnden utgår analysen vid det inledande stadiet utifrån följande:

- Att nämnden vidtar effektiva åtgärder för lagefterlevnad;
- Den praktiska möjligheten för de registrerade att utöva sina rättigheter;
- Att nämnden får bättre kontroll på sina informationstillgångar.

Denna analys består utav följande fyra kapitel:

1. Bakgrund;
2. Metod;
3. Åtgärdslista;
4. Slutsats.

Tabellerna i avsnitt *"3. Åtgärdslista"* är indelade i prioriteringsordning (låg, medel och hög). Åtgärdslistan är tillställd hela nämnden.

3. ÅTGÄRDSLISTA

Åtgärder av hög prioritet

Risk	Nuläge	Åtgärd
Utbildning		
En förutsättning för att dataskyddsarbetet ska fungera effektivt i nämnden är att samtliga medarbetare i nämnden har viss kunskap om de skyldigheter som följer av Dataskyddsförordningen. Kontinuerliga utbildningsinsatser är därför en viktig del i arbetet med Dataskyddsförordningen. Avsaknaden av kontinuerlig utbildning till samtliga medarbetare kan leda till brister vid hanteringen av personuppgifter.	Utbildningsinsats har utförts av dataskyddsombudet om registerförteckningar. Medarbetare har fått information GDPR i början av GDPR:s i ikraftträdande.	Ta fram en utbildningsplan för dataskyddsarbete innehållandes en målsättning för att tillförsäkra att samtliga medarbetare besitter kunskap inom de grundläggande bestämmelserna i Dataskyddsförordningen. Utbildningsplanen ska särskilt fokusera på utbildning av nyanställda medarbetare, men bör även inkludera regelbundna insatser för att hålla en jämn kunskapsnivå hos samtliga medarbetare. Dataskyddsombudet kan vara behjälpligt med att ta fram utbildningsmaterial och genomföra utbildningsinsatser.
Registerförteckning		
En förutsättning för att man som personuppgiftsansvarig ska vara complient med dataskyddslagstiftningen är ett man har en registerförteckning (artikel 30-register) på plats. Registerförteckningen är ett levande dokument som ska uppdateras löpande i takt med att nya personuppgiftsbehandlingar införs i verksamheten eller att vissa personuppgiftsbehandlingar upphör. Att upprätta en registerförteckning är både tids- och resurskrävande, men det är ett arbete som behöver prioriteras då förteckningen	Dataskyddsombudet har fått information om att arbetet med nämndens artikel 30-register har påbörjats. Nämnden ska endast sammanställa materialet innan det initiala arbetet med artikel 30-registret är avklarat.	Inkom med ert artikel 30-register till dataskyddsombudet när detta är färdigställt.

utgör en grundbult i den dokumentation som varje personuppgiftsansvarig är skyldig att ta fram enligt lagstiftningen.		
Systematiskt arbete med dataskydd		
För att uppfylla de skyldigheter som Dataskyddsförordningen uppställer är arbetet med dataskydd något som nämnden måste ägna sig åt löpande. Avsaknaden av kontinuerliga processer och etablering av riktlinjer och rutiner i nämnden leder till att systematiska processer för fortsatt arbete stannar av.	Inför Dataskyddsförordningens ikraftträdande skedde en större insats. För att nämna några exempel: Information lämnades om GDPR för ledningsgruppen, kontaktpersoner utsågs som skulle arbeta med Dataskyddsförordningen och Workshop hölls där inbjudna kunde ställa frågor om Dataskyddsförordningen och höra andras frågor.	Dataskyddsombudet upplever att det systematiska arbetet med dataskyddsfrågor avstannat något vid upprättandet av artikel 30-register. Viktigt är att redan nu fastställa vilka steg som kommer härnäst i processen efter att artikel 30-registert är på plats. Dataskyddsombudet föreslår att nästa steg bör vara utbildningsinsatser och att implementera dataskyddsombudets åtgärdslista.
Förankring av dokumentation och skriftlig dokumentation		
För att uppfylla de skyldigheter som Dataskyddsförordningen uppställer är arbetet med dataskydd något som organisationen måste ägna sig åt löpande. Avsaknaden av kontinuerliga processer och etablering av riktlinjer och rutiner i organisationen leder till att systematiska processer för fortsatt arbete stannar av.	Kommunövergripande dokumentation om Dataskyddsförordningen finns på Insidan. Nämnden har även tillgång till samarbetsrum där SKR:s information om Dataskyddsförordningen sprids. Inga nämndspecifika riktlinjer eller rutiner har tagits fram.	Nämnden bör undersöka om det finns ett behov av att upprättat nämndspecifika riktlinjer och rutiner om hantering av personuppgifter i Arbetsmarknadsnämnden. Nämnden bör även undersöka hur dokumentation bättre kan förankras i hela nämnden. En påminnelse om att läsa igenom den information som finns på insidan bör skickas till nämndens medarbetare.

Åtgärder av medel prioritet

Risk	Nuläge	Åtgärd
Löpande arbetet med artikel 30-register		
Eftersom registerförteckningen är ett levande dokument som ska uppdateras löpande i takt med att nya personuppgiftsbehandlingar införs i verksamheten eller att vissa personuppgiftsbehandlingar upphör måste artikel 30-registret uppdateras löpande.	Nämnden saknar utarbetad och skriftlig rutin för översyn/uppdatering av artikel 30-registret. Avsaknaden av detta kan innebära en risk att registret över tid tappar relevans och inte återspeglar nämndens personuppgiftsbehandlingar.	Utarbeta och implementera en rutin för att registerförteckningen ska uppdateras så fort en ny behandling har identifierats eller när en befintlig behandling förändras. Även en översyn av registerförteckningen bör ske ett par gånger årligen. Dataskyddsombudet bör också, vid behov, vara delaktigt i arbetet med registerförteckningar i syfte att bistå nämnden vid eventuella frågor om inmatningar i artikel 30-registret.

Åtgärder av lägre prioritet

Risk	Nuläge	Åtgärd
Spridning av information		
Om personuppgifter lagras på flera olika ställen av flera olika personer riskerar personuppgifter att spridas och nämnden kan då förlora kontrollen över sina informationstillgångar.	Lagring förekommer på olika ställen i exempelvis mailen.	Implementera en rutin om att en översyn ska göras inom ett visst tidsintervall över vissa lagringsutrymmen, såsom mailen. Detta för att säkerhetsställa att dokument innehållandes personuppgifter läggs i korrekt mapp, ärendehanteringssystem eller annan lämplig och korrekt lagringsyta alternativt gallras/raderas.

4. SLUTSATS

Dataskyddsombudet har noterat att nämnden har kommit en bra väg på implementeringsarbetet av Dataskyddsförordningen, där en del insatser vidtagits för att efterleva Dataskyddsförordningen. Därefter har en första inventering och kartläggning av nämndens personuppgifter skett. Utifrån det håller nämnden på att producerat en registerförteckning (artikel 30-register). För att inte tappa fart i implementeringsprocessen uppmanar dataskyddsombudet emellertid nämnden att gå vidare till nästa steg i implementeringsprocessen och att även fastställa fler steg. Eftersom registerförteckningen är ett sådant dokument som ständigt är under arbete är det viktigt att inte fastna vid detta första implementeringssteg. Dataskyddsombudets rekommendation är därför att fortgå med övriga steg i implementeringsprocessen och inrätta en rutin som möjliggör fortsatt arbete med registerförteckningen parallellt med övriga steg i implementeringsprocessen. Av rutinen bör det framgå att när en ny behandling uppstår, eller när en förändring identifieras av befintliga behandlingar som nämnden utför, ska dessa registreras i registerförteckningen.

För att uppnå en tillfredsställande nivå av dataskydd i nämnden är det en förutsättning att dataskyddsarbetet implementeras i det vardagliga arbetet. I dataskyddsombudets uppdrag ingår att påpeka att fortsatta satsningar för att öka kunskapsnivån i nämnden är nödvändiga för att säkerställa en god nivå av dataskydd i hela nämnden. För att förhindra att dataskyddsarbetet blir passivt efter att den inledande implementeringsperioden har passerat, är dataskyddsombudet av uppfattningen att dataskydd bör inkluderas i nämnden arbetsprocess i hela verksamheten. För att tillförsäkra att dataskyddsarbetet kontinuerligt förbättras och följs upp i hela organisationen är det därför viktigt att nämnden arbetar kontinuerligt och systematiskt med dataskyddsfrågor.

Dataskyddsombudets personuppgiftsrevison har mynnat ut i ett antal förbättringsåtgärder. Dessa anges under rubriken "*3. Åtgärdslista*" och utgör dataskyddsombudets bedömning av vilka åtgärder som är nödvändiga i nuläget, baserat på granskat underlag inför personuppgiftsrevisionen samt intervjuer. Vid det fortsatta arbetet bör en riskbaserad metod användas vilket innebär att "högrisk-åtgärder" (rödmarkerat) i första hand bör åtgärdas.

Uppsala kommun

Datum:
2020-12-18

Diarienummer:
KRN-2020-00054

KOMMUNREVISIONEN

Mottagare:

Kommunstyrelsen

Kommunfullmäktige, för kännedom

Förstudie: Arbetet med införandet av GDPR inom Uppsala kommun

Uppsala kommuns revisorer har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts i Uppsala kommun och därvid bilda sig en uppfattning om nuläget. Uppdraget ingår i revisionsplanen för år 2020.

Kommunen har generellt sett tagit sig an frågorna kring skyddet av person-uppgifter på ett föredömligt sätt och beaktat de centrala delarna av GDPR, även om fullständigt behandlingsregister på processnivå behöver färdigställas inom delar av kommunens organisation, vilket är ett pågående arbete. Åtgärder har vidtagits genom att utbilda medarbetare för att säkerställa att medvetenhets- och kunskapshöjande insatser kring personuppgiftsbehandlingar.

Kommunen har en tydlig struktur med roller och ansvar som för att fortsätta med dataskyddsarbetet och har utöver ett externt upphandlat dataskyddsombud dessutom tillsatt dataskyddssamordnare i varje förvaltning.

Koncernledningsgruppen har intresse av utvecklingen av dataskyddsarbetet och dataskydd är på agendan. Dessutom sker ett aktivt arbete kring digital trans-formation där ostrukturerad data hanteras.

Bedömningen baserat på den översiktliga förstudie som genomförts är att ett starkt arbete anpassning efter GDPR har utförts, med förbättringspotential på vissa delar.

För kommunrevisionen

Per Davidsson

Per Davidsson, ordförande

Postadress: Uppsala kommun, kommunrevisionen, 753 75 Uppsala
Telefon: 018-727 11 32 (Kansli)
E-post: kommunrevisionen@uppsala.se
www.uppsala.se

Arbetet med införandet av GDPR inom Uppsala kommun - en förstudie och nulägesbeskrivning

Linus Owman

Omid Asali

pwc

Innehåll

1. Inledning

1.1 Bakgrund - GDPR

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), innebär en skärpning av dataskyddslagstiftningen inom EU, både avseende organisationers åtaganden och de registrerade individernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare. För att den ska respekteras införs möjligheten till kraftfulla sanktioner för de organisationer som ignorerar eller brister i att uppfylla de nya kraven. Sanktionsnivåerna har valts så att de ska vara avskräckande och för att det inte ska löna sig att bryta mot reglerna för att spara pengar. Väsentliga sanktionsavgifter för bristande efterlevnad, upp till 20 miljoner kronor, kan utfärdas för myndigheter. Det införs också en rätt för privatpersoner att kräva skadestånd av de organisationer som inte tillhandahåller deras rättigheter enligt förordningen. Förordningen började tillämpas den 25 maj 2018.

Förordningen innehåller nya krav jämfört med Personuppgiftslagen, som exempelvis att alla organisationer själva har en skyldighet att bedöma riskerna för att de registrerades integritet kränks samt vidta lämpliga åtgärder för att minska dessa risker. Organisationer måste även i vissa fall utse dataskyddsombud och rapportera allvarliga personuppgiftsincidenter till tillsynsmyndigheten (och i vissa fall de berörda registrerade) inom 72 timmar. Om organisationen misstänker att någon personuppgiftsbehandling kan medföra höga integritetsrisker för de registrerade måste man göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador.

I slutet av juni detta år (2020) publicerade tidningen "Aktuell Säkerhet" en debattartikel kring införandet av GDPR och aktuellt läge. Några korta citat hjälper till att belysa denna förstudies aktualitet ytterligare:

"Efter en förhållandevis lugn start slogs det i mars i år rekord i antal utfärdade böter inom ramarna för GDPR. Idag, när digitaliseringen ute på företagen går ännu snabbare i svallvågorna av den globala pandemin är det absolut nödvändigt att företag inte bara förstår det ansvar de har över sina kunders data, utan att de i samma snabba takt utvecklar sitt dataskydd och säkerhetsarbete. .../.../... För små och medelstora företag är de potentiella konsekvenserna svårare att överblicka. De har i regel stramare budgetar och mindre IT-avdelningar och riskerar att bli överväldigade av de resurser och de insatser som krävs för ett fullgott dataskydd. Att samtidigt säkerställa efterlevnad av GDPR gör situationen än mer komplicerad. Det finns gott om åtgärder som kan vidtas utan stor budget. Att investera i lösningar för dataskydd och strategier är en grundläggande del i att framtidssäkra en verksamhet i en digital värld. Kort sagt – dataskydd behöver vara en central del i verksamhetens affärsstrategi – inte minst i takt med att IT-sidan blir alltmer komplex." [1]

[1] https://www.aktuellsakerhet.se/gdpr-fyller-tva-hur-har-det-gatt/

1.2 Syfte och frågeställning

Uppsala kommuns revisorer har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts i Uppsala kommun och därvid bilda sig en uppfattning om nuläget. Förstudien ingår i revisionsplanen för år 2020.

Frågeställningen för denna förstudie är således: *"Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?".*

Frågeställningen ovan har besvarats genom en gruppintervju. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter
- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

1.3 Avgränsning och metod

Förstudien syftar inte till att kartlägga *de facto* efterlevnad av direktivet, då detta skulle ha mer av en granskande karaktär, dvs falla utanför ansatsen hos en förstudie. Förstudien har fokuserat på att ge en generell bild av hur arbetet genomförts och fortskrider, utan att detaljerade studier genomförts på förvaltningsnivå. Översiktliga dokumentstudier har genomförts.

Intervju har således genomförts med personer som representerar de funktioner med ett särskilt ansvar i införandet av GDPR. Intervju har genomförts i gruppform tillsammans med CIO Thomas Ekvall, chefsjurist Lena Grapp, biträdande jurist Simon Elfstadius, informationssäkerhetsstrateg/CISO Robert Reineck, IT-strateg Johan Olofsson och en separat intervju med extern upphandlad dataskyddsombud JP Infonet - Laura Gashi.

2. Kartläggning

2.1 Bakgrund - införandet av GDPR

Arbetet med införandet av GDPR inom Uppsala kommun initierades före årsskiftet 2017 där ett projekt med en projektledare initierades. Projektet arbetade fram vilka åtgärder som skulle vidtas med projektplan och listor. Projektet avslutades 2019 med kvarvarande restlistor, även om stora delar av projektet hade gjort framsteg. Kommunen anställde en biträdande jurist under 2018 med ett särskilt fokus på GDPR. Chefsjuristen agerade som dataskyddsombud för alla nämnder i kommunen fram tills dess att Uppsala kommun upphandlade JP Infonet som dataskyddsombud.

Stadsdirektören tog 2018 ett beslut för att Uppsala kommun samordnat skulle arbeta med informationssäkerhetsfrågor, vilket resulterat i inrättandet av en funktion för informationssäkerhet med representation från flertalet stödjande verksamheter. Funktionen, som leds av informationssäkerhetsstrategen, har varit bärande och koordinerade i hanteringen för att successivt avveckla projektets restlistor.

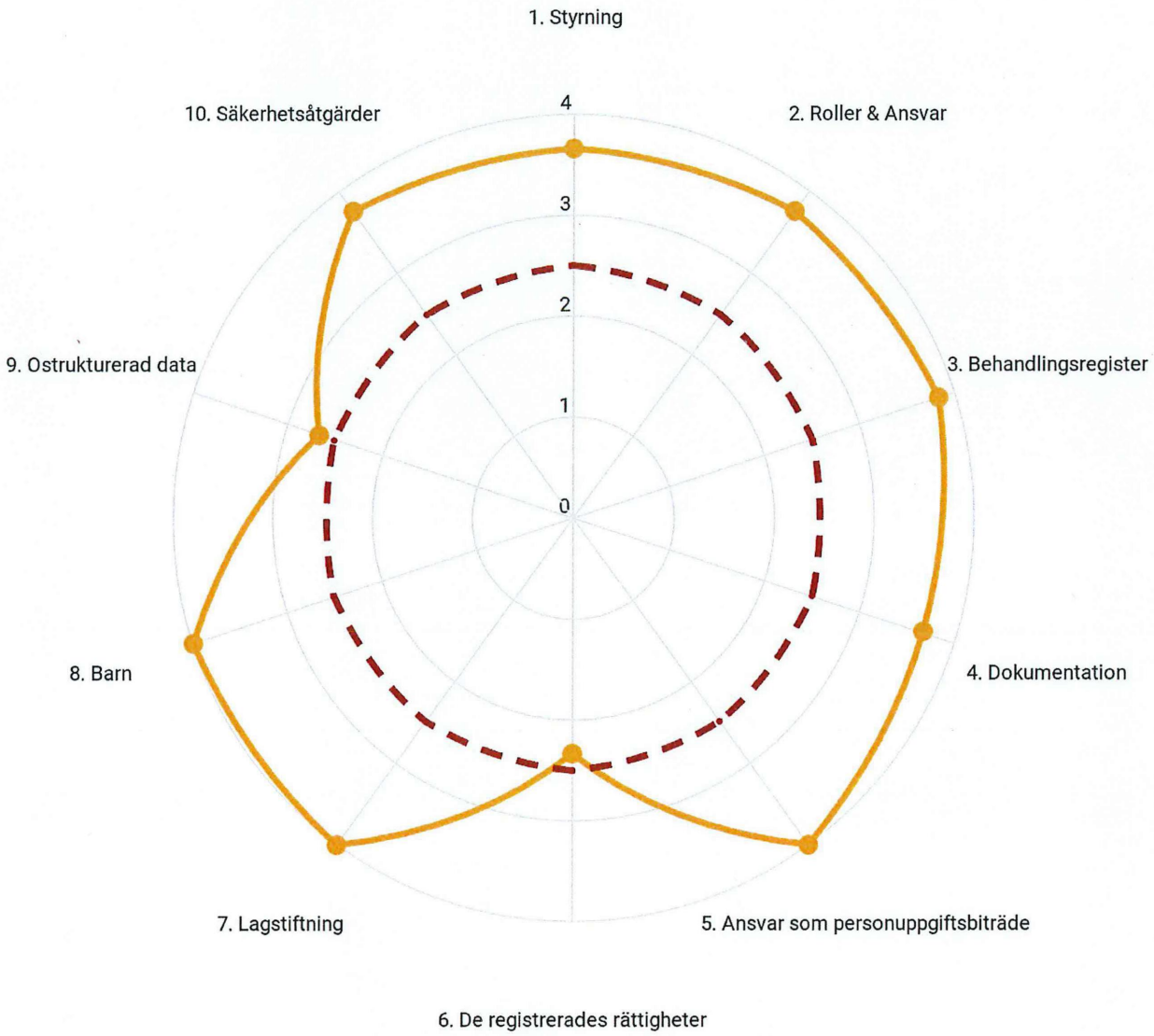
Arbetet av GDPR efterlevnad fortskrider idag där CIO är med i koncerngruppen och koncernledningsgruppen, och där ett flertal av Uppsala kommuns funktioner aktivt arbetar med GDPR och dess efterlevnad.

2.2 Övergripande resultat

För att sammanställa denna rapport har PwC intervjuat relevanta personer med insyn i Uppsala kommuns dataskyddsarbete och det anpassningsarbete som gjorts till GDPR.

Diagrammet nedan visar resultatet av vår genomgång. Diagrammet är baserat på intervjusvar till 35 standardiserade frågor och ger en översiktsbild av alla relevanta områden för korrekt hantering av personuppgifter.

Den orangea linjen representerar Uppsala kommuns resultat. Den röda prickade linjen utgör grundvärde för vad vi bedömer är ett godkänt dataskyddsarbete. Medelvärdet för detta är 2,5. Värdet är baserat på en generell bedömning utifrån intervjuformulärets svarsalternativ. Alternativ 1,0 innebär att kommunen inte påbörjat något arbete alls inom området och alternativ 4,0 innebär i korthet att kommunen infört en fullständig (och ofta automatiserad) process kring behandling. Ett värde på 2,5 innebär således att organisationen ligger över både 1,0 (inget gjort) och 2,0 (lite gjort) och tangerar 3,0 (vidtagit åtgärder).



Den sammanfattande bedömningen är att Uppsala kommun har vidtagit välriktade åtgärder med att ta sig an de utmaningar som den nya dataskyddsförordningen innebär. Vidare arbetar Uppsala kommun aktivt och strukturerat med dataskyddsförordningen idag tillsammans med JP Infonet som dataskyddsombud. kommunen ligger i helhet en bra bit över den nivå som vi betraktar som grundnivå, dock så ser vi förbättringspotential på område 6, "de registrerades rättigheter". I den fortsatta rapporten går vi djupare in på varje områden och ger specifika rekommendationer.

3. Resultat

3.1 Styrning

Kommunens resultat för området är **3,7 av 4,0**. Det har funnits ett tydligt uppdrag att införa GDPR från ledningsgruppen. Arbetet har sedan drivits framåt av chefsjurist, CIO, biträdade jurist, informationssäkerhetsstrateg/CISO, IT-strateg, dataskyddsombud och de dataskyddssamordnare som numera utsetts inom varje nämnd. Idag drivs arbetet vidare av ovan nämnda funktioner samt av säkerhetsavdelningen, kommunikationsavdelningen, HR, IT-säkerhet och stadsarkivet.

Beslutet till att etablera dataskyddssamordnare för varje nämnd, grundades i ett behov att förlägga arbetet med GDPR närmare respektive verksamhet och personuppgiftsansvarig (PUA). Utöver detta arbetar dataskyddsombudet och dataskyddssamordnarna, tillsammans med juridik och CISO, nära varandra med efterlevnad av dataskyddsförordningen. Ambitionen är att vara ett kraftfullt kunskapsnätverk för Uppsala kommun. Dataskyddsombudet har genom utbildningsaktiviteter höjt medvetenheten kring dataskyddsförordningen och har ombett dataskyddssamordnarna att upprätta fullständiga listor gällande artikel 30. Då det krävs tid och förståelse för att kvalitativt utföra arbetsuppgifterna är det viktigt att förvaltningsledningen kommunicerar prioriteringen.

Dataskyddsfrågan är på agendan i kommunledningen och koncernledningsgruppen, och det är inom kommunledningen som beslutet att tillsätta dataskyddssamordnare har verkställts. Vidare ska lägesbilden samt arbetet med GDPR och informationssäkerhet regelbundet diskuteras med Stadsdirektören. Riktlinjer kring hantering av Informationssäkerhet har utarbetats på kommunstyrelsenivå.

Uppsala kommun har under projektet utfört systeminventeringar på nämndsnivå, med syfte att skapa artikel 30-register. Idag driver dataskyddsombudet och dataskyddssamordnarna ett arbete med att göra en förnyad inventering av behandlingar på processnivå. Anledning till detta beslut är önskan om att få ett mer heltäckande artikel 30-register utgående från processer.

Uppsala kommun har valt att använda sig av SKR:s "klassa" som verktyg för informationssäkerhetsklassificering där konsekvenser bedöms utifrån bristande konfidentialitet, tillgänglighet och riktighet. För andra året i rad ingår det i internkontrollplanen att granska att alla IT-stöd är klassificerade, att ett systematiskt arbete utförs med objekten, och att Uppsala kommun fortsätter med det framgent. De intervjuade anser att klassificering av IT-stöd är långt gånget, men att systematiken med åtgärdsplaner kan förbättras.

3.2 Roller och ansvar

Inom området roller och ansvar har kommunen erhållit resultatet **3,8 av 4,0**. Kommunen har utvärderat om en roll som dataskyddsombud är nödvändigt och landat i ett formellt beslut tillämpa en sådan roll för Uppsala kommun. Syftet med ett dataskyddsombud anses vara att ha en koordinerande roll som bidrar med kompetensutväxling och ett större nätverk inom ämnet av dataskydd. Rollen som dataskyddsombud har upphandlats externt och utförs nu av JP Infonet. För att dataskyddssamordnarna ska ha en tydlig roll inom Uppsala kommun

har en promemoria som underlag på koncernledningsnivå använts för att tydligt definiera rollen.

Ansvaret för kommunövergripande system är en diskussion som fortsatt utreds idag, där definiering av hur ansvaret bör se ut i framtiden utreds. Nämnderna är ansvariga för personuppgiftsbehandlingarna som sker inom respektive nämnd. Detta ansvar regleras i reglementet där nämnderna är definierade som ansvariga för sin information och verksamhet. I reglementet definieras arbetsformer, arbetsområdet samt personansvarsområdet. Dataskyddsombudet planerar en genomgång av alla nämnder i närtid.

En granskning av efterlevand har idag inte genomförts av dataskyddsombudet, men anges vara pågående. De granskningsaktiviteter som hittills genomförts utgörs av en skrivbordsövning där dokumentationen inom kommunen granskats. Det planeras en tillsyn av GDPR-efterlevand där brister och förbättringar kommer att rapporteras.

3.3 Behandlingsregister (registerförteckning)

För detta område har kommunen erhållit ett resultat på **3,8 av 4,0**. Varje nämnd arbetar fram ett eget behandlingsregister, eftersom varje nämnd är personuppgiftsansvarig enligt kommunens sätt att definiera detta. Just nu är Uppsala kommun i en transformeringsfas där karaktär av fokus för behandlingsregister ändras. Tidigare har fokus i behandlingsregistret varit behandlingar per system, och förändringen innebär att nämnderna istället definierar innehållet i behandlingsregister per process och behandling. Denna aktivitet är prioriterad. Vid den planerade inventeringen kommer personkategorier att kartläggas och analyseras.

Behandlingsregister hanteras idag i Excel (SKR:s mall) även om systeminköp har varit på agendan. Om en konsekvensanalys behöver utformas i relation till en behandling utförs det i en annan Word-mall. Det finns tydlig vägledande dokumentation för hur processen ska genomföras och dokumenteras. Inom dataskyddsförordningen är frågan om vilka personkategorier som behandlas en av de mest komplexa. Dataskyddsombudet bidrar med stöd och en funktionsbrevlåda har tillämpats.

Om personuppgifter förs över till mottagare i andra organisationer så regleras det i PUB-avtal. Detta gäller även om personuppgifter skickas utanför EU/EES. De intervjuade menar att många PuB-avtal tecknats, även om några saknas. Oftast handlar det i dessa fall om att avtalsvillkoren inte har godkänts sinsemellan avtalsparterna. Detta är en pågående process och målet är att ha PUB-avtal på plats för alla relationer där detta är aktuellt.

När det gäller radering och gallring av personuppgifter omfattas Uppsala kommun av offentlighetsprincipen och således bevaras det mesta av personuppgifter som har behandlats. Det finns dokumenthanteringsplaner i verksamheten idag kring hur vissa kategorier av personuppgifter ska gallras. I de enskilda fall när individer ber om gallring behöver Uppsala kommun granska huruvida de, med hänsyn till andra regulatoriska åtaganden, kan tillgodose individens rättighet eller inte.

3.4 Dokumentation

Inom frågeområdet för dokumentation ligger kommunen på **3,7 av 4,0**.

I nuläget finns det en informationstext kring personuppgiftsbehandlingar ("behandling av personuppgifter") riktad till kommuninvånarna för Uppsala kommun på hemsidan. En integritetspolicy för intern hantering av personuppgifter inom Uppsala kommun saknas dock idag. Detta beror på ett aktivt val från kommunens sida att inte ha policyer som säger att organisationen förbinder sig att följa lagen, vilket huvudsyftet med en sådan policy har ansetts vara. Däremot beskrivs behandlingen av den anställdes personuppgifter enligt GDPR i anställningsbeviset.

Rutiner som är mer specifikt än integritetspolicyn kring hur Uppsala kommun hanterar personuppgifter idag finns i artikel 30 registret just nu. Enligt dataskyddsombudet kommer en utvärdering kring registrerades rättigheter att genomföras.

Den mall som används för personuppgiftsbiträdesavtal och som är standard inom Uppsala kommun är den mall som SKR har tillhandahållit. Biträdade jurist har bistått med rådgivning när nämnderna har varit i behov av att utföra en konsekvensanalys för en specifik behandling.

3.5 Ansvar som personuppgiftsbiträde

Kommunen hamnar här på **4,0 av 4,0**. Det finns ett flertal situationer där Uppsala kommun agerar personuppgiftsbiträde åt en annan organisation. Det finns exempelvis idag system som sköts centralt av Uppsala kommun, och som även bolagen använder.

För externa utförare inom exempelvis äldreomsorg finns tydligt ansvar definierat. Även om Uppsala kommun rekommenderar SKRs mall för PuB-avtal som standard, så finns det situationer där Uppsala kommun använder biträdesavtal som Inera tillhandahåller avseende behandlingar av personuppgifter i HSA-katalogen. De intervjuade menar att många PuB-avtal tecknats, även om några saknas. Oftast handlar det i dessa fall om att avtalsvillkoren inte har godkänts sinsemellan avtalsparterna. Detta är en pågående process och målet är att ha PUB-avtal på plats för alla relationer där detta är aktuellt.

De intervjuade menar på att SKRs uppfattning har varit att man inte ska behöva interna PuB-avtal mellan nämnderna, utan att detta ska regleras sinsemellan i reglementet.

Dataskyddsombudet kommer att i sin tillsynsrapport att analysera situationen för Uppsala kommun och komma med förslag på åtgärdslista. Tillsynsrapporten kommer att baseras på det som har definierats i behandlingsregistret av nämnderna och bolagen. Dock så kan denna kartläggningen vara bristande idag då den interna gränsdragningen inte har varit självklar. De kommunala bolagen har idag inte upprättat PUB-avtal med kommunens IT-stab i de fall IT-staben är personuppgiftsbiträde till den personuppgiftsansvariga styrelsen.

3.6 De registrerades rättigheter

För frågeområdet kring de registrerades rättigheter hamnar kommunen på **2,3 av 4,0**. Resultatet speglar avsaknaden av dokumenterade processer i form av styrdokument för att uppnå de registrerades rättigheter.

Kommunen har information på hemsidan kring hur behandlingen av personuppgifter sker och var den registrerade kan vända sig med frågor. Varje nämnd har också ansvar att informera om hur personuppgifter behandlas.

Om en registrerad person åberopar en rättighet har Uppsala kommun tillgängliga mallar för den registrerade där efterfrågan kan göras åt egna vägnar eller i vägnar för en annan registrerad. Det finns inte en formaliserad process i styrdokument där det beskrivs tillvägagångssättet för att tillgodose en registrerad persons rättigheter. Styrdokument där hantering av registrerades rättigheter beskrivs kommer att formuleras längre fram. Den informella processen är att den registrerade efterfrågar uppgifter från olika nämnder som sedan går till IT för analys. Detta är en helt manuell process idag.

Arbetssättet kring arbetssätt kring hur registerutdrag lämnas ut, hur rättning eller radering av felaktiga personuppgifter är delvis dokumenterat, bland annat via delegationsordning.

På uppsala.se får besökarna en beskrivning om att hemsidan hanterar cookies med tillhörande länk där alla cookies tydligt beskrivs.

Inom försörjningsstöd finns det en robot som hanterar kontrollslagningar gentemot externa system. Dock så sker inget automatiskt beslutsfattande, och inte heller någon annanstans inom kommunen, varför detta är en rättighet som den registrerade inte kan åberopa (dvs rättigheten att inte utsättas för automatiserat beslutsfattande). Denna fråga utgick därför ur frågebatteriet och drabbar inte poängsättningen inom detta område negativt. De intervjuade är intresserade av frågan men är begränsade då kommunallagen inte tillåter automatiska beslut.

Rekommendationer:

- Färdigställ styrdokument för hur de registrerades rättigheter kan tillgodoses.
- Dokumentera processen för hur registerutdrag lämnas ut, samt hur rättning eller radering av felaktiga personuppgifter sker.

3.7 Lagstiftning

Kommunen hamnar här på **4,0 av 4,0**. Uppsala kommun har ingen utpekad funktion för omvärldsbevakning, dock så faller det naturligt inom relevant funktion. Juristavdelningen bevakar Riksdagens hemsida och utredningar. CISO och IT-strateg inom Uppsala kommun bevakar även området inom ramen för sitt nätverk. Dataskyddsombudet håller sig också uppdaterad genom att följa lagstiftning och domar, vilket utgör en del av rollbeskrivningen.

3.8 Barn

Kommunen hamnar här på **4,0 av 4,0**. Kommunen behandlar med lagstadgad grund personuppgifter om barn. Uppsala kommun klassificerar barns uppgifter som hög risk och vidtar de säkerhetsåtgärder som är nödvändiga och som ligger i linje med SKRs rekommendationer.

3.9 Ostrukturerad data

Avseende området ostrukturerad data är resultatet att kommunen ligger på **2,7 av 4,0**. Utvärdering av ostrukturerad data gjordes inom ramen för GDPR projektet inför införandet av GDPR i kommunen, och verksamheten granskade området. De intervjuade försöker att inte göra skillnad på "ostrukturerad data" och annan data, utan istället förtydliga behovet av att beskriva personuppgiftsbehandlingar och säkerställa GDPR oavsett lagring eller IT-stöd.

Ostrukturat material ligger sparat på olika filytor för olika typer av behandlingar. När det gäller ostrukturerat material med känslig information och sekretessmarkerade uppgifter är organisationens hållning i intervjuer att filytor och e-post bör undvikas. Uppsala kommun har i form av policy för digital transformation och policykartläggning påbörjat arbetet med att etablera rutiner som resulterar i minimering av behandling av ostrukturerat material. Det finns en vägledning för digital arbetsplats och att information skall hanteras i verksamhetssystemen och mindre på filytor. Ett tillvägagångssätt för Uppsala kommun är Office365 plattformen där taggning av personnummer kan appliceras.

Rekommendation:

- Fullfölj kartläggningen av förekomsten av ostrukturerad data och tillsätt nödvändiga åtgärder för att minska användningen av denna typ av data.
- Säkerställ vidare att medarbetarna utbildas kring hur minskning av användningen av ostrukturerad data kan uppnås.

3.10 Säkerhetsåtgärder

Inom området säkerhetsåtgärder får kommunen **3,8 av 4,0**. Uppsala kommun har arbetat med att klassa sin information med stöd av verktyget SKR-KLASSA. Det kommunen anser att de har kommit längst med är att inom ramen för IT-upphandlingar gå igenom och klassificera upphandlingsvillkoren för IT-stödet. I den projektmodell som tillämpas inom kommunen har kommunen fångat upp relevanta frågor inom säkerhetsåtgärder i checklistor. Detta har varit ett särskilt initiativ för det arbete som sker för den digitala transformationen där regulatoriska frågor i processer som dataskydd och dataskydd som standard bearbetas.

Kommunen har genomfört utbildning för informationssäkerhet som har varit riktad mot informationsägare. Dataskyddsombudet har också genomfört kompetenshöjande insatser gentemot samma grupp. Dock så finns det inget gemensamt utbildningsmaterial tillgängligt för på Uppsala kommun. Detta kommer att ändras då ett verktyg är upphandlat och utbildningspaketet är inom informationssäkerhet.

Kommunen har en tydlig process för konsekvensbedömningar kopplat till specifika personuppgiftsbehandlingar. Kontinuerligt stöd ges till verksamheten kring processen.

Uppsala kommun har en tydlig process och rutin för hur personuppgiftsincidenter skall hanteras. Enligt dataskyddsombudet som har detaljerad insyn i hur kommuner arbetar med dataskyddsfrågor, anses Uppsala kommun vara en av de kommuner som har uppmärksammat många incidenter. De intervjuade hävdar att de positiva synergierna med uppmärksammade incidenter i verksamheten resulterar i ökad medvetenhet och kunskap. Dataskyddsombudet blir inblandad i varje personuppgiftsincident. Denna process finns tillgänglig för alla medarbetare på intranätet Insidan. Processen innebär att ett formulär fylls i som skickas till dataskyddsombudet, som stöttar PUA i att fatta beslut om huruvida

incidenten bör rapporteras vidare till Datainspektionen. Kommunen anser att kompetenshöjande åtgärder kring upptäckandet av incidenter behöver bli bättre framöver. Det är IT-support och verksamheten som har dialog och utredning när en incident anses inträffa. Processen har funnits på plats i knappt ett år och mindre justeringar har gjorts under tiden. Uppsala kommun använder dataskyddsombudet ofta och rutinmässigt vilket bidrar med att många frågor hanteras.

4. Slutsatser

Inledningsvis ställdes frågan *"Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?"* Frågeställningen har besvarats genom ett intervjuformulär som besvarats genom intervjumetodik. Intervjuer har genomförts i gruppform med representanter från de delar av kommunen som anses vara representativa för kommunens arbete med GDPR. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter
- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

Svaret på frågeställningen om huruvida *"ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna"* får besvaras med "Ja". Liksom inom andra områden finns det alltid utrymme för förbättringar och ett fåtal rekommendationer har föreslagits i föregående avsnitt.

Kommunen har generellt sett tagit sig an frågorna kring skyddet av personuppgifter på ett föredömligt sätt och beaktat de centrala delarna av GDPR. Ett fullständigt behandlingsregister på processnivå behöver dock färdigställas inom delar av kommunens organisation, vilket är ett pågående arbete. Åtgärder har vidtagits genom att utbilda medarbetare för att säkerställa medvetenhets- och kunskapshöjande insatser kring personuppgiftsbehandlingar.

Kommunen har en tydlig struktur med roller och ansvar för att fortsätta med dataskyddsarbetet och har utöver ett externt upphandlat dataskyddsombud dessutom tillsatt dataskyddssamordnare i varje förvaltning. Koncernledningsgruppen har vidare intresse av utvecklingen av dataskyddsarbetet och dataskydd är på agendan. Dessutom sker det ett aktivt arbete kring digital transformation där ostrukturerad data hanteras.

Bedömningen baserat på den översiktliga förstudie som genomförts är att ett starkt arbete anpassning efter GDPR har utförts, med förbättringspotential på vissa delar.

Beslutet att tillsätta ett dataskyddsombud har inneburit att det löpande arbetet med att övervaka efterlevnaden inom området har prioriterats i den dagliga verksamheten, detta utförs tillsammans med verksamheten, främst tillsammans med funktionerna för juridik och IT.

"Dataskyddsförordningen (The General Data Protection Regulation) är till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter."

Datainspektionens hemsida