Datum
2022-03-29

Adress

Diarienummer
SN-2022-211

Yttrande

Till
Stadsrevisionen

Granskning av dataskyddsarbete
SR-2021-93

Servicenämnden beslutade den 29 mars 2022 att lämna följande yttrande:

Sammanfattning

EY har på uppdrag av Malmö stadsrevision granskat efterlevnaden av dataskyddsförordningen GDPR. Syftet med granskningen har varit att bedöma om kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden säkerställer ett ändamålsenligt dataskyddsarbete.

Den samlade bedömningen är att det finns en övergripande organisation och arbetsgång med tillhörande roller samt rutiner för risk- och sårbarhetsanalyser och riktlinjer för personuppgifts-incidenter, men att kommunstyrelsen och de granskade nämnderna inte i tillräcklig utsträckning har säkerställt att dataskyddsarbetet bedrivs ändamålsenligt.

Servicenämnden välkomnar denna rapport och instämmer i flera delar med revisionen. Servicenämnden anser sig bedriva ett aktivt dataskyddsarbete och det finns god medvetenhet om det arbete som ska göras, men delar revisionens rekommendationer gällande att det behövs mer resurser, fler nedtecknade rutiner samt att arbetet med att ta fram riskanalyser och konsekvensbedömningar brister och behöver prioriteras. I rapporten ges ett antal generella rekommendationer till kommunstyrelsen och nämnderna samt ett antal riktade rekommendationer till servicenämnden. I yttrandet anges dessa rekommendationer tillsammans med kommentarer samt förslag på åtgärder från nämnden.

Yttrande

EY har på uppdrag av Malmö stadsrevision granskat efterlevnaden av dataskyddsförordningen GDPR. Syftet med granskningen har varit att bedöma om kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden säkerställer ett ändamålsenligt dataskyddsarbete.

Den samlade bedömningen är att det finns en övergripande organisation och arbetsgång med tillhörande roller samt rutiner för risk- och sårbarhetsanalyser och riktlinjer för personuppgiftsincidenter, men att kommunstyrelsen och de granskade nämnderna inte i

tillräcklig utsträckning har säkerställt att dataskyddsarbetet bedrivs ändamålsenligt. Bedömningen grundar sig på att kommunstyrelsen och nämnderna inte säkerställt att riskanalyser och konsekvensbedömningar genomförs på ett strukturerat sätt, samt att registerförteckningarna är kompletta. Kommunstyrelsen och nämnderna saknar tillräckliga kontroller, uppföljning och rapportering av dataskyddsarbetet. Utbildningsinsatserna för samtliga anställda är otillräckliga. Det saknas ett systematiskt arbete som säkerställer en god kunskapsnivå avseende dataskydd och informationssäkerhet.

Servicenämnden välkomnar denna rapport och instämmer i flera delar med revisionen. Servicenämnden anser sig bedriva ett aktivt dataskyddsarbete och det finns god medvetenhet om det arbete som ska göras, men delar revisionens rekommendationer gällande att det behövs mer resurser, fler nedtecknade rutiner samt att arbetet med att ta fram riskanalyser och konsekvensbedömningar brister och behöver prioriteras. I rapporten ges ett antal generella rekommendationer till kommunstyrelsen och nämnderna samt ett antal riktade rekommendationer till servicenämnden. Nedan anges dessa rekommendationer tillsammans med kommentarer från förvaltningen samt förslag på åtgärder.

Inledande rekommendationer som riktar sig till kommunstyrelsen och övriga nämnder

Rekommendation 1: Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen.
Utöver de stadsövergripande styrdokument som tagits fram av stadskontoret gällande dataskydd har servicenämnden tagit fram ett flertal själva där vi har sett ett behov av att komplettera. Dessa styrdokument informeras kontinuerligt om vid utbildningstillfällen och på intranätet. Servicenämnden instämmer dock i att det är viktigt att också kontinuerligt granska och följa upp att dessa styrdokument efterlevs. Servicenämnden genomför ett antal granskning- och uppföljningsåtgärder årligen, men har inget dokumenterad plan kring detta arbete. Servicenämnden ämnar under 2022 att ta fram en sådan plan som kommer att fungera som ett årshjul för dataskyddsarbetet där olika granskning- och uppföljningsåtgärder kommer vara återkommande. I denna plan kommer granskning och uppföljning av bland annat registerförteckning, incidentrapportering och systemdokumentation ingå.

Rekommendation 2: Tillse att ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.
Servicenämnden förstår utifrån rapporten som att denna rekommendation rör ansvarsfördelningen inom staden. Servicenämnden delar revisionens bild till viss del och upplever framför allt att det kan uppstå vissa frågor om ansvar vid stadsövergripande personuppgiftsbehandlingar, till exempel vid personuppgiftsincidenter och vid avtal med personuppgiftsbiträden. Samtidigt har Stadskontoret har tagit fram flertalet rutiner inom dataskyddsarbetet som hanterar frågan om ansvarsfördelning inom staden och servicenämnden ser gärna att stadskontoret fortsätter detta arbete inom så många delar som

möjligt så att vi får en enhetlig hantering i staden. Servicenämnden bedömer att det internt inom förvaltningen finns en tydlig ansvarsfördelning där dataskyddssamordnaren och informationsäkerhetssamordnaren samordnar, följer upp och granskar dataskydds- och informationssäkerhetsarbetet samt håller utbildningar, rådger och stöttar vid behov. Till hjälp finns ett dataskyddsnätverk som består av dataskyddskoordinatorer på de olika avdelningarna som fungerar som stöd ute i verksamheterna, tar emot rapporter om personuppgiftsincidenter och uppdaterar avdelningens registerförteckning.

Efterföljande rekommendationer till kommunstyrelsen och övriga nämnder

Rekommendation 1: Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data.
Stadskontoret har tagit fram en stadsövergripande rutin ”Rutin för inventering och klassificering av informationstillgångar i Malmö stad” som täcker både strukturerad och ostrukturerad data. Servicenämnden bedömer att eventuella förtydliganden av klassificering av ostrukturerad data bör framgå av denna rutin framför att varje nämnd tar fram egna kompletteringar förutom i de fall då det finns ostrukturerad data som är förvaltningsspecifik.

Rekommendation 2: Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.
Inom servicenämnden ansvarar varje avdelning för att deras registerförteckning, genom dataskyddskoordinatorn, är uppdaterad och riktig. Till stöd för detta finns dataskyddssamordnaren som ger råd och stöd kring hur registerförteckningen ska fyllas i, eller om det finns några övriga frågor. Servicenämnden tagit fram ett eget formulär på intranätet där medarbetare kan gå in och anmäla när de har startat en ny personuppgiftsbehandling. Detta formulär togs fram just för att det inte skulle ta för lång tid för personuppgiftsbehandlingar att läggas till i registerförteckningen, till exempel när registerförteckningen ses över två gånger om året. Gällande kontinuerliga granskningar av registerförteckningarna instämmer servicenämnden med revisionen att det inte finns en dokumenterad rutin för detta. Servicenämnden ämnar åtgärda detta under 2022 genom den plan för granskning och uppföljning som redogjordes för under rekommendation 1 under de inledande rekommendationerna till kommunstyrelsen och övriga nämnder.

Rekommendation 3: Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.
Att säkerställa att personuppgifter endast behandlas för de ändamål som de samlas inför är en grundläggande förutsättning för korrekt personuppgiftsbehandling enligt GDPR. Detta är något som tas upp vid varje utbildningstillfälle gällande dataskydd. De aktiva rutiner som servicenämnden har för att i största möjliga mån säkerställa detta innefattar att påminna om rutinen att personuppgiftsbiträdesavtal ska bifogas till alla avtal där personuppgifter kommer att behandlas för att på så sätt säkerställa att våra avtalsparter inte missbrukar de personuppgifter som servicenämnden ansvarar för. Servicenämnden har redan påbörjat ett arbete med att se över instruktionsbilagan till PUB-avtal med syftet att tydliggöra

personuppgiftsavtalsförhållandet mellan servicenämnden och avtalspart. Bland annat kommer instruktionen uppdateras med en passage om att servicenämnden ska ha avstämningar med avtalspart där avtalspart åläggs att redogöra för hur de säkerställer att personuppgifter endast behandlas för de ändamål de samlas in för.

Vidare genomför servicenämnden utifrån dokumenterad rutin loggkontroller, bland annat i systemet Pro Capita som används inom färdtjänst. Detta görs för att kontrollera att uppgifter inte används av obehöriga eller används för annat än ändamålet med behandlingen. Servicenämnden håller också på att se över ytterligare möjligheter till loggkontroller i andra system.

Rekommendation 4: Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.
Servicenämnden hänvisar här till svaret i föregående rekommendation.

Rekommendation 5: Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.
Servicenämnden delar inte fullt ut revisionens bedömning gällande servicenämndens incidenthanteringsrutin. Servicenämnden har valt att ta fram en egen incidenthanteringsrutin framför att följa stadens just med syftet att öka kontroll och att incidenthanteringsrutinen efterlevs i praktiken. Servicenämnden upplevde att det fanns risker med stadens rutin gällande att rapporterade incidenter inte nådde fram till dataskyddsamordnaren inom den tidsfrist på 72 timmar som gäller för att rapportera till tillsynsmyndighet. Servicenämnden har därför infört en rutin där medarbetare rapporterar direkt till dataskyddskoordinator på sin avdelning som tar kontakt med dataskyddssamordnare för att göra en initial bedömning om incident ska rapporteras till tillsynsmyndighet. I samband med detta blir även chef informerad om incidenten och är även den som tar det slutgiltiga beslutet om en incident ska rapporteras till tillsynsmyndighet eller inte enligt beslutad delegationsordning. Denna rutin finns även nedtecknad på serviceförvaltningens intranät.

Servicenämnden har även arbetat in sin personuppgiftsincidenthantering inom den generella avvikelsehanteringen och flera verksamheter inom serviceförvaltningen har valt personuppgiftsincidenter som avvikelser som de ska arbeta särskilt inriktat med under 2022. Dataskyddssamordnaren utbildar också kontinuerligt om vikten av personuppgiftsincidentrapportering och det har även gett utslag i rapporteringen då vi såg en tydlig ökning under 2021. Personuppgiftsincident-statistik rapporteras även till den politiska nämnden genom årsanalysen.

Inledande rekommendationer till servicenämnden:

Rekommendation 1: Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.

Servicenämnden delar revisionens bild av att det har saknats rätt förutsättningar att strukturerat genomföra riskanalyser och konsekvensbedömningar. Redan innan dataskyddsgranskningen identifierade dataskydds- och informationsäkerhetssamordnaren på servicenämnden detta som en prioriterad fråga inför 2022. Ett arbete har redan påbörjats med att ta fram en mall för att dessa analyser och bedömningar ska kunna genomföras, frågan har lyfts i förvaltningens ledningsgrupp och det kommer även att hållas utbildningar i hur dessa mallar ska fyllas i. Servicenämnden har en långsiktig vision med detta arbete där tanken är att de ifyllda analyserna och bedömningarna ska vara levande dokument som ses över vid uppgradering eller andra systemförändringar. Inledningsvis kommer de system som innehåller de mest känsliga personuppgifterna prioriteras för att säkerställa att dessa system lever upp till de dataskyddskrav som åligger personuppgiftsansvarig. Servicenämnden är dock medvetna om att det kommer krävas mycket resurser och tid inledningsvis för att komma i gång med detta arbete och att det finns en resurs- och kompetensbrist som behöver hanteras. Det är sedan viktigt att detta arbete blir en naturlig del av verksamheternas system- och personuppgiftshantering och att förvaltningen tillser att det finns resurser tillgängliga som kontinuerligt arbetar med dessa frågor vilket inte är fallet idag.

Rekommendation 2: Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid.

Servicenämnden delar revisionens uppfattning att det här är ett grundläggande krav på personuppgiftsansvarig och anser att ämnet är besvarat under rekommendation 2 under efterföljande rekommendationer till kommunstyrelsen och övriga nämnder.

Rekommendation 3: Tillse att systemägare har den kunskap och tid som krävs för att utföra ålagda arbetsuppgifter.

Systemägare uppdateras med jämna mellanrum på ledningsgruppsmöten om aktuella dataskyddsfrågor och vid deltagande på dataskyddsutbildningar. Det redan nämnda arbetet med riskanalyser och konsekvensbedömningar kommer att kräva systemägares aktiva deltagande då det är de som kommer att godkänna konsekvensbedömningar med tillhörande föreslagna riskåtgärder. Även systemägare kommer därför få en utbildning gällande detta arbete.

Rekommendation 4: Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.

Servicenämnden instämmer i bilden att det inom vissa delar av dataskyddsarbetet saknas resurser, huvudsakligen inom arbetet med att ta fram riskanalyser och konsekvensbedömningar för system samt upprätthålla generell informationssäkerhet knutet till IT-system. Serviceförvaltningen kommer att genomgå en omorganisation under 2022 där en central IT-enhet kommer att bildas. Till denna enhet kommer 2–3 systemförvaltare att anställas vilket kommer att skapa bättre förutsättningar för ovan nämnda dataskyddsarbete. Förvaltningen arbetar även med att banta ner antalet system genom att använda färre system som kommer att kunna utföra samma tjänster. Samtidigt är det viktigt att lyfta fram att omorganisationen kommer att ta tid och att arbetet med att säkerställa att det finns

tillräckligt med resurser är ett långsiktigt arbete, men samtidigt ett prioriterat sådant inom dataskyddsarbetet.

Efterföljande rekommendationer till servicenämnden

Rekommendation 5: Utarbeta dokumenterade rutiner som säkerställer att gallring av personuppgiftsbehandlingar verkställs inom satt tidsram.
Som tidigare nämnt kommer dataskyddssamordnaren och informationsäkerhetssamordnaren att ta fram en dokumentmall där konsekvensbedömningar och informationssäkerhets-riskanalyser ska genomföras innan en personuppgiftsbehandling påbörjas. I detta dokument kommer även ytterligare en del kopplas på som hanterar gallringsrutiner. Syftet är att arkivarien alltid ska vara delaktig vid upphandling av nytt system och att gallringsrutiner ska tas fram samt att gallringsbeslut ska tas, såsom att tillse att behandlingen täcks av förvaltningens arkivredovisning.

Rekommendation 6: Utarbeta dokumenterad rutin för hur behörighetskontroller ska genomföras i servicenämndens IT-system.
Servicenämnden har redan som ett resultat av intern kontroll-granskningen ”Felaktig tillgång till information och lokaler” planerat att ta fram en rutin som beskriver hur behörigheter till IT-stöd ska hanteras. Denna kommer att tas fram under 2022. Rutinen kommer att inkludera ett konkret arbetsunderlag för chefer vid hantering av behörigheter som inte är kopplade till stadens katalogtjänst. Samtidigt arbetar nämnden aktivt med att byta ut föråldrade system mot nya system där behörigheten kopplas till stadens katalogtjänst vilket kommer att underlätta hanteringen av behörigheter och öka informationssäkerheten.

Ordförande

Jan Olsson (S)

Nämndsekreterare

Johanna Beckmann