Datum
2022-12-07

Adress

Diarienummer
SN-2022-211

Yttrande

Till
Stadsrevisionen

Granskning av dataskyddsarbete
SR-2021-93

Servicenämnden föreslås besluta att lämna följande yttrande:

Sammanfattning
Serviceförvaltningen har under 2022 arbetet aktivt med att genomföra de åtgärder som servicenämnden beslutade om i sitt yttrande till stadsrevisionen. Ett viktigt perspektiv som anlagts på detta arbete har varit att skynda långsamt i den mening att arbetet ska bära frukt långsiktigt och bli en integrerad del av förvaltningens processer för kvalitativt och rättsenligt arbete. Avsikten har inte varit att ”bocka av” åtgärder utan ta fram rutiner och processer som ska säkerställa att hanteringen av personuppgifter följer dataskyddsförordningens föreskrifter år ut och år in. Personalomsättningar tillsammans med försenade rekryteringar på kansli- och utvecklingsavdelningen har dock medfört att förvaltningen inte har nått ända fram till målsättningen för året gällande dataskydd, men grunden är lagd för att ta vidare arbetet under 2023.

Det uppföljande yttrandet är upplagt utifrån de åtgärder som presenterades i föregående yttrande med redogörelse för om och hur genomförande har skett.

Yttrande
Serviceförvaltningen har under 2022 arbetet aktivt med att genomföra de åtgärder som servicenämnden beslutade om i sitt yttrande till stadsrevisionen. Ett viktigt perspektiv som anlagts på detta arbete har varit att skynda långsamt i den mening att arbetet ska bära frukt långsiktigt och bli en integrerad del av förvaltningens processer för kvalitativt och rättsenligt arbete. Avsikten har inte varit att ”bocka av” åtgärder utan ta fram rutiner och processer som ska säkerställa att hanteringen av personuppgifter följer dataskyddsförordningens föreskrifter år ut och år in. Personalomsättningar tillsammans med försenade rekryteringar på kansli- och utvecklingsavdelningen har dock medfört att förvaltningen inte har nått ända fram till målsättningen för året gällande dataskydd, men grunden är lagd för att ta vidare arbetet under 2023.

Nedan redogörs för de åtgärder som nämnden beslutade om 2022-03-29, §34, genomförandet av dessa samt hur effekterna av åtgärderna ska tas hand om. Åtgärderna är uppradade utifrån prioriteringsgraden som stadsrevisionen angav på sina rekommendationer:

- gemensamma inledande rekommendationer till kommunstyrelsen och övriga nämnder
- gemensamma efterföljande rekommendationer till kommunstyrelsen och övriga nämnder
- inledande rekommendationer specifikt för servicenämnden
- efterföljande rekommendationer specifikt för servicenämnden

Inledande rekommendationer till kommunstyrelsen och övriga nämnder

Rekommendation 1: Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen.

Beslutad åtgärd av servicenämnden: Ta fram en plan som ska fungera som ett årshjul för granskning- och uppföljningsåtgärder.

Åtgärden är genomförd. Förvaltningen har tagit fram en dokumenterad rutin för uppföljning och granskning av förvaltningens dataskyddsarbete där granskning- och uppföljningsåtgärder inom ett antal dataskyddsområden anges. Rutinen innehåller dels åtgärder som ska vara återkommande varje år, dels anger den att det varje år ska genomföras särskilda punktinsatser. Återkommande åtgärder kommer vara uppföljning av konsekvensbedömningar/riskanalyser av systemstöd som hanterar personuppgifter, uppföljning av personuppgiftsbiträdesavtal, uppföljning av nämndens registerförteckningar samt sammanställning och rapportering av personuppgiftsincidenter. Även öppna grundläggande utbildningar om dataskydd och informationssäkerhet som hålls av dataskyddssamordnaren och informationssäkerhetssamordnaren kommer att vara återkommande inslag. Särskild punktinsats under 2022 var att föra över registerförteckningar från Excel-dokument till systemstödet Ifacts, en insats som genomfördes i hela staden utifrån stadskontorets ledning.

Tillsammans med rutinen tog förvaltningen även fram ett årshjul för att illustrera planerade åtgärder 2022 vilket förvaltningen kommer att göra i början på varje år. Det finns även en ambition från centralt håll i staden att ta fram ett stadsövergripande årshjul för dataskyddsarbetet och då kommer serviceförvaltningen anpassa sitt utifrån det för att bidra till ett harmoniserat dataskyddsarbete i staden där synkade åtgärder kan leda till erfarenhets- och kunskapsutbyte.

Rekommendation 2: Tillse att ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.

Ingen åtgärd beslutad av servicenämnden

Den stadsövergripande ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är en fråga som stadskontoret äger. Gällande den interna ansvarsfördelningen hos serviceförvaltningen konstaterade nämnden till stadsrevisionen att förvaltningen hade en etablerad 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. Denna ansvarsfördelning framgår av sidor på förvaltningens intranät. Förvaltningen valde dock att som en ytterligare åtgärd ta fram en dokumenterad ansvarsfördelning som även förtydligade informationsägares ansvar.

Efterföljande rekommendationer till kommunstyrelsen och övriga nämnder

Rekommendation 1: Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data.

Ingen åtgärd beslutad av servicenämnden

Som nämnden angav i sitt ursprungliga yttrande till stadsrevisionen så har stadskontoret tagit fram en stadsövergripande rutin *"Rutin för inventering och klassificering av informationstillgångar i Malmö stad"* som täcker både strukturerad och ostrukturerad data. Servicenämnden gjorde därför bedömningen att eventuella förtydliganden av klassificering av ostrukturerad data borde framgå av denna rutin framför att varje nämnd tog fram egna kompletteringar förutom i de fall då det finns ostrukturerad data som är förvaltningsspecifik. Någon sådan data har förvaltningen inte identifierat och förvaltningens ambition är att ostrukturerad data ska undvikas i den mån det går.

Rekommendation 2: Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.

Beslutad åtgärd av servicenämnden: Genom plan för granskning och uppföljning av arbetet med dataskyddsförordningen tillgodose uppföljning av registerförteckningens riktighet och fullständighet över tid.

Som tidigare nämnt genomfördes ett stort arbete i staden då alla registerförteckningar flyttades från Excel till systemstödet Ifacts. Genom att använda systemstöd underlättas arbetet med att säkerställa registerförteckningarnas riktighet och uppföljning genom att det dels går att avgränsa vilka svar som kan anges, dels att det går att följa upp när förteckningen och dess behandlingar senast uppdaterades. En konsekvens av överflyttningen var dock att det tillkom fält där information ska anges som inte fanns med i de ursprungliga Excel-filerna vilket innebar att inga förteckningar var fullständiga. På servicenämnden arbetar vi med att komplettera denna information och samtidigt se över övrig angiven information i registerförteckningen. Detta arbete samordnas av dataskyddssamordnaren med hjälp av dataskyddskoordinatorerna. Under 2022 har förvaltningen även haft hjälp av en praktikant

som har hjälpt till att komplettera med standardiserad information som gick förlorad i migreringen.

Utifrån den beslutade åtgärden kommer servicenämnden som tidigare nämnt att ha uppföljning av registerförteckning som en återkommande åtgärd i förvaltningens årshjul för dataskyddsarbete. Den samordnas av dataskyddssamordnaren som med hjälp av koordinatorer ute på avdelningarna kontaktar ägare för personuppgiftsbehandlingar för att se över om information är riktig och uppdaterad.

Rekommendation 3: Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.

Beslutade åtgärder av servicenämnden:
1. Se över instruktionsbilaga till personuppgiftsbiträdesavtal.
2. Ta fram rutiner för loggkontroller.

Den första åtgärden kommer att redovisas i nästa avsnitt eftersom det mer direkt behandlar frågan om personuppgiftsbiträdesavtal.

Den andra åtgärden är påbörjad, men kommer även fortsätta in på 2023. Sedan tidigare har servicenämnden en dokumenterad rutin för loggkontroll i systemstödet Pro Capita som används inom färdtjänst och dessa utförs enligt rutin. Under året har förvaltningen även tagit fram en rutin för loggkontroll i stadens ärendehanteringssystem Platina där fokus kommer ligga på ärenden som är markerade med sekretess och/eller känsliga personuppgifter. Vidare har en arbetsgrupp påbörjat ett arbete för att ta fram en rutin för loggkontroll i kontaktcenters ärendehanteringssystem Artvise. Syftet med dessa loggkontroller är att identifiera om det finns någon oregelbunden eller omotiverad aktivitet kring ärenden som kan antyda att obehörig har tagit del av information i ett ärende. Arbetet med att ta fram systemspecifika rutiner för loggkontroll kommer att fortsätta under 2023.

Rekommendation 4: Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.

Beslutad åtgärd av servicenämnden: Se över instruktionsbilagan till PUB-avtal för att öka möjligheter till kvalitetskontroll av leverantörer.

Förvaltningen såg under 2022 ett behov av att ta ett större omtag kring mallen för PUB-avtal utöver att bara se över instruktionsbilagan. Dataskyddssamordnaren fick signaler från medarbetare på förvaltningen att stadens rutin gällande PUB-avtal och de överenskommelser som finns för stadens interna biträdesrelationer, alltså när en förvaltning är biträde till en annan förvaltning, var otydliga och det fanns en osäkerhet kring när respektive mall skulle användas och hur de skulle fyllas i. Serviceförvaltningen har därför tagit fram en intern rutin

för PUB-avtal som anger när PUB-avtal ska användas, hur de ska fyllas i och vad som behöver göras om avtal med leverantör berör flera nämnder. Servicenämnden är ägare för flera system där det kan finnas fler personuppgiftsansvariga än servicenämnden och då är det viktigt att se till att ansvarsfördelningen blir tydlig. I samband med detta har även instruktionsbilagan förtydligats så att det är tydligt för personuppgiftsbiträdet vad den får och inte får göra samt att det tydligt framgår den personuppgiftsansvarige har rätt att göra olika former av kontroller för att säkerställa att personuppgiftsbiträdet uppfyller kraven enligt dataskyddsförordningen.

Som tidigare nämnt har också förvaltningen lagt in som en del av sin årliga uppföljning och granskning att förvaltningen ska se över vilka leverantörer som hanterar personuppgifter och om det finns PUB-avtal med dessa.

Rekommendation 5: Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.

Ingen åtgärd beslutad av servicenämnden
Servicenämnden bedömde att de hade en tillräcklig kontroll över att incidenthanteringen efterlevs i praktiken vilket även har visat sig under 2022. Förvaltningen har ett kontinuerligt inflöde av personuppgiftsincidenter utspritt på flera verksamheter. Det finns en medvetenhet på förvaltningen att personuppgiftsincidenter ska anmälas även om de kan framstå som ofarliga eller lösta eftersom de kan bidra till förvaltningens kvalitetsutvecklingsarbete genom att rutiner ses över och kvalitetskontrolleras. Under 2022 har också verksamheterna kontaktcenter och ITD på egna initiativ i samråd med dataskyddssamordnaren sett över incidenthanteringsrutiner för att tydliggöra gränsdragningar gentemot andra nämnder samt göra processen så användarvänlig som möjligt.

Inledande rekommendationer till servicenämnden

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

Beslutad åtgärd av servicenämnden: Ta fram en mall för konsekvensbedömning och igångsätta ett arbete med att dokumentera behandlingar i våra system i prioriterad ordning.
Servicenämnden har under 2022 tagit fram en mall för konsekvensbedömning samt ett stöddokument för hur mallen ska fyllas i. Mallen har kvalitetskontrollerats av stadens dataskyddsombud och förvaltningen har tagit fram en förteckning över de system som ska prioriteras. På grund av tidigare nämnda omständigheter gällande personalomsättningar har dock förvaltningen inte kommit så långt i detta arbete som planerat. Hitintills har kontaktcenters och intern kundtjänsts upphandling av nytt ärendehanteringssystem genomgått konsekvensbedömningar, men planen var att alla system med känsliga personuppgifter på förvaltningen skulle ha konsekvensbedömts. Förvaltningen har dock en ambition att detta ska vara genomfört vid årets slut. Genomförda konsekvensbedömningar

ska ses över en gång om året för eventuella revideringar, ett arbete som samordnas av dataskyddsamordnaren. Under 2023 kommer förvaltningen att fortsätta konsekvensbedöma de system som inte hunnits med eller prioriterats under 2022.

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

Beslutad åtgärd av servicenämnden: Genom plan för granskning och uppföljning av arbetet med dataskyddsförordningen tillgodose uppföljning av registerförteckningens riktighet och fullständighet över tid.
Här hänvisar nämnden till redogörelsen under rekommendation 2 under avsnittet *Efterföljande rekommendationer till kommunstyrelsen och övriga nämnder.*

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

Beslutad åtgärd av servicenämnden: Förvaltningen ska uppdatera ledningsgruppen med jämna mellanrum gällande dataskyddsarbetet samt utbilda systemägare gällande konsekvensbedömning.
I slutet på detta år kommer dataskyddssamordnaren att redogöra för ledningsgruppen, som är förvaltningens systemägare, årets dataskyddsinsatser med fokus på konsekvensbedömningar och systemägares ansvar. På grund av tidigare nämnd personalomsättning och prioriteringar har ledningsgruppen inte fått den utbildning och återkommande uppdatering kring dataskyddsarbetet som önskats, men avsikten är att det ska vara på plats från 2023 så att de är uppdaterade och insatta kring sitt ansvar.

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

Beslutad åtgärd av servicenämnden: Förvaltningen kommer genomgå en omorganisation och bilda en IT-enhet och därmed få ett mer samlat grepp om systemhanteringen.
Förvaltningens omorganisation med en central IT-enhet på kansli- och utvecklingsavdelningen blev försenad på grund av att rekrytering av chef behövde göras om. IT-enheten kom inte i gång förrän i augusti i stället för maj som planerat. Enheten har sedan den bildades arbetat med att kartlägga befintlig kompetens för att identifiera vilka resursbehov som finns och tagit fram en handlingsplan med ett förslag på systemförvaltarmodell för förvaltningen. Förslaget kommer att presenteras inom kort för ledningsgruppen som kommer att besluta i rekryteringsfrågan.

Efterföljande rekommendationer till servicenämnden

Rekommendation 5: Utarbeta dokumenterade rutiner som säkerställer att gallring av personuppgiftsbehandlingar verkställs inom satt tidsram.

Beslutad åtgärd av servicenämnden: Ta fram mall för konsekvensbedömning och i detta arbete engagera arkivarie för att säkerställa att gallringsrutiner följs.
Under 2022 har förvaltningen varit utan arkivarie i 6 månader på grund av att rekrytering fick göras om vilket har hämmat förvaltningens möjligheter att arbeta med gallringsrutiner. Förvaltningen har dock som tidigare nämnt tagit fram mall för konsekvensbedömning där gallringsfrågor ska utredas och tanken är även att arkivarie, informationssäkerhetssamordnare och dataskyddssamordanare under 2023 ska ta ett gemensamt grepp kring gallringsrutiner, med fokus på avveckling av system, men även processer gällande initiering av personuppgiftsbehandlingar.

Rekommendation 6: Utarbeta dokumenterad rutin för hur behörighetskontroller ska genomföras i servicenämndens IT-system.

Beslutad åtgärd av servicenämnden: Ta fram rutin för hantering av behörighet till system.
Förvaltningen har tagit fram en rutin för avslut av behörigheter som tar särskilt sikte på avslut av behörigheter som inte är kopplade till medarbetarens AD, alltså behörigheter som inte är beroende av att medarbetaren har ett användarkonto genom sin anställning. Det är beslutat att vid varje avslutsmöte med chef ska medarbetare ange i en förteckning av system som ej är kopplade till AD vilka den har behörighet till så att chef kan meddela om avslut. På detta vis minimeras risken att medarbetare har obehörig tillgång efter att de har lämnat sin anställning. Samtidigt fortsätter förvaltningens arbete med att byta ut äldre system mot nya där en del av kravställningen kommer att vara att behörigheten går genom stadens AD.

Ordförande

Jan Olsson (S)

Nämndsekreterare

Jim Johannesson

[Här anger du om det finns reservationer/särskilda yttranden]