Datum
2022-02-28

Adress
August Palms Plats 1

Diarienummer
STK-2022-148

Yttrande

Till
Revisorskollegiet

Rapport från revisorskollegiet - Granskning av dataskyddsarbete
SR-2021-93

Sammanfattning
Med anledning av rubricerad granskningsrapport lämnar kommunstyrelsen följande synpunkter. Kommunstyrelsen framhåller att det av revisionsrapporten framgår att kommunstyrelsen uppvisar goda ambitioner till fortsatt utveckling av dataskyddsarbetet. Kommunstyrelsen delar revisionens bedömning att arbetet med dataskyddet behöver stärkas ytterligare.

Revisionen bedömer att det finns en god förståelse för informationsklassificering och riskarbete men att det saknas en rutin för att säkerställa regelefterlevnad över tid. Det finns dock en rutin för informationsklassificering som möjliggör regelefterlevnad över tid.

Det pågår ett arbete med att utveckla systemstödet Ifacts för handläggning av registerförteckningen i syfte att möjliggöra en mer systematisk uppföljning av dataskyddsarbetet. Att utveckla systemstödet kommer på sikt att leda till en bättre kontroll över pågående personuppgiftsbehandlingar och uppföljning utifrån kraven i dataskyddsförordningen. I detta arbete inkluderas utveckling av befintlig mall för konsekvensbedömningar och tillhörande rutin.

Vad avser frågan om tillräckliga resurser för att säkerställa att det finns reella möjligheter att bedriva ett effektivt dataskyddsarbete har det på stadskontoret initierats en utredning som ska syfta till att kartlägga resursbehovet utifrån ett dataskydds-och informationssäkerhetsperspektiv. Inom ramen för denna utredning kommer rollerna kopplat till dataskyddsarbetet att definieras och förtydligas och bland annat tjäna som underlag för att ytterligare säkerställa dataskyddsombudets oberoende inom ramen för sin tillsynsfunktion och motverka intressekonflikter.

En rutin för att säkerställa att riktlinjer och styrdokument förblir riktiga över tid kommer att implementeras för att tillse dels dokumentens förenlighet med befintlig organisationsstruktur dels förenlighet med lagstiftningen på området.

Möjligheten att centralt förse Malmö stads samtliga anställda med utbildning i dataskydd via en kommungemensam plattform undersöks och förväntas på sikt ge ökade möjligheter att kommunövergripande och på bredare front nå ut med utbildningar i dataskydd och informationssäkerhet samt ge förutsättningar till både kontroll och uppföljning vad avser den grundläggande kompetensen inom dataskydd. I detta sammanhang ska framhållas att nätverksträffar avseende dataskydd bedrivs regelbundet på central nivå i syfte att kompetensförsörja förvaltningarna i sitt arbete med dataskyddet. Det finns således en etablerad form för kompetensutveckling av medarbetare i staden via nyssnämnda nätverk.

Vidare kommer befintliga krav för behörighetstilldelning och uppföljning av loggar att ses över inom ramen för det övergripande informationssäkerhetsarbetet inom staden.

Yttrande

Nedan redovisas granskningsrapportens samtliga rekommendationer var för sig i anslutning till de åtgärder som kommunstyrelsen/stadskontoret avser genomföra och förväntad effekt av åtgärderna. Samtliga åtgärder ska, såvida inte annat anges, vara genomförda senast i slutet av 2023.

Rekommendation (1)

Utarbeta en tydlig plan för granskning och uppföljning av dataskyddsförordningen.

Åtgärd

Kommunstyrelsen föreslås uppdra åt stadskontoret att ta fram en tydlig plan för granskning och uppföljning av dataskyddsförordningen.

Förväntad effekt

Att ett mer effektfullt dataskyddsarbete vad avser regelefterlevnad uppnås på sikt. Genom denna åtgärd skapas en formell struktur för uppföljning av arbetet med dataskyddsförordningen vilket skapar en kontinuitet och en god överblick av arbetet inom respektive förvaltning och staden som helhet.

Rekommendation (2)

Tillse att ansvarsfördelningen kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.

Åtgärd

Förtydliga ansvaret kopplat till de definierade rollerna inom ramen för befintliga styrdokument. En utredning avseende resurskartläggning på området för dataskydd och informationssäkerhet har initierats på stadskontoret, se STK-2022-55. Inom ramen för utredningen ses rollerna kopplat till ansvarsfördelningen över som en del i den allmänna resurskartläggningen inom områdena informationssäkerhet- och dataskydd.

Förväntad effekt

Att organisationen får klart för sig när respektive roll ska involveras och under vilka steg i processen. Vidare blir effekten en tydligare struktur för dataskyddsarbetet där innehållet för respektive roll klart framgår och en ökad effektivitet i det dagliga dataskyddsarbetet främjas.

Den utredning som nämns ovan förväntas ge svar på vilka resurser som behövs för att ytterligare stärka kommunstyrelsens förutsättningar att fullfölja sitt uppdrag inom informationssäkerhet och dataskydd.

Rekommendation (3)
Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data. Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.
Åtgärd
Det finns en rutin och ett protokoll för att klassa enskilda handlingstillgångar. Detta görs dock inte i Ifacts i dagsläget. Rutinen och det nya klassningsprotokollet kommer att ses över och kommuniceras ut till hela organisationen.
Det finns en skriftlig instruktion för handläggning av registerförteckningar, se ”instruktion för handläggning av registerförteckningar version 1.0 2018-09-18”.
Stadskontoret har vidare påbörjat ett utvecklingsarbete kopplat till Ifacts vilket är ett system som bland annat används för att klassa, kravställa och följa upp informationshanteringen. Detta utvecklingsarbete inbegriper hela staden. Utvecklingen av Ifacts innebär vidare en förbättrad möjlighet att följa upp pågående personuppgiftsbehandlingar men också att nya personuppgiftsbehandlingar handläggs mer effektivt genom de funktionella möjligheter som följer av systemstödet i jämförelse med den handläggning som idag sker i excelfiler. Utvecklingsarbetet syftar till att registerförteckningarna framöver ska kunna handläggas i Ifacts.
Förväntad effekt
Att tillkommande såväl som redan registrerade personuppgiftsbehandlingar kommer att handläggas mer effektivt, särskilt med avseende på uppföljning genom de inbyggda möjligheterna i systemstödet.

Rekommendation (4)
Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för
Åtgärd
Möjligheten att genomföra utbildningsinsatser på central nivå undersöks och arbetet med utbildningsinsatser internt på stadskontoret är under uppbyggnad. Vidare pågår ett arbete med att utveckla registerförteckningen i systemet Ifacts.
Förväntad effekt
Att en ökad medvetenhet om och en fördjupad förståelse för ändamålets centrala betydelse för personuppgiftsbehandlingar uppnås över tid vilket motverkar risken för att personuppgifter behandlas för andra ändamål än de ursprungligen samlats in för. Arbetet med att utveckla verktyget för registerförteckningen förväntas bidra till att det blir enkelt att göra rätt och följa dataskyddslagstiftningen över tid och till förbättrade möjligheter att kvalitetssäkra personuppgiftsbehandlingar bland annat utifrån kravet på ändamålsbegränsning.

Rekommendation (5)
Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.
Åtgärd
Uppföljning av biträdesrelationer och ingångna personuppgiftsbiträdesavtal genom verktyget för registerförteckningar i Ifacts. Utveckla den systematiska kontrollen över ingångna personuppgiftsbiträdesavtal genom Ifacts.
Förväntad effekt
Att uppföljning och granskning av ingångna personuppgiftsbiträdesavtal kommer kunna företas mer systematiskt och inom ramen för det uppföljningsarbete som kan göras med registerförteckningen som grund.

Rekommendation (6)
Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.
Åtgärd
Utbildningsinsatser planeras att vidtas i syfte att höja den allmänna medvetenheten kring vad som kan utgöra en personuppgiftsincident i dataskyddsförordningens mening. Vidare kommer de anställda genom utbildningsinsatser att medvetandegöras om rutinens existens.
Förväntad effekt
En ökad förståelse för vad en personuppgiftsincident är, vilka bedömningar som ska göras och hur en personuppgiftsincident ska hanteras rent praktiskt i organisationen samt ytterst en ökad medvetenhet om rutinens existens. Åtgärden kommer sannolikt att öka den faktiska efterlevnaden av rutinen.

Rekommendation (7)
Säkerställa att styrdokument förblir riktiga och aktuella över tid.
Åtgärd
Säkerställa att styrdokumenten förses med datum för när de har upprättats, ägare samt uppgift om när de senast ska revideras.
Förväntad effekt
Att en systematisk kontroll över styrdokumentens riktighet och aktualitet över tid uppnås.

Rekommendation (8)
Utarbeta instruktioner till systemägare för hur behörighetskontroller ska genomföras.
Åtgärd
Befintliga krav för behörighetstilldelning och uppföljning av loggar ses över i samband med att IT:s kravbibliotek integreras i Ifacts, se s. 7 under ”åtgärdsområde 5” i kommunstyrelsens yttrande i ärende STK-2021-158 avseende revisorskollegiets granskning av IT-säkerheten i Malmö stad.
Förväntad effekt
Att bättre styrning för behörighetskontroller och loggar uppnås.

Rekommendation (9)
Säkerställa att utbildningar inom dataskyddsarbetet genomförs regelbundet för kommunens samtliga anställda utefter en dokumenterad utbildningsplan.
Åtgärd
Stadskontorets HR-avdelning har påbörjat en utredning avseende upphandling av en stadsövergripande digital läroplattform. En sådan lösning möjliggör både utbildning i form av e-utbildningar och uppföljning av vilka medarbetare som genomgått utbildning i dataskydd.
Förväntad effekt
Kompetenshöjande för Malmö stads samtliga anställda vad avser den allmänna förståelsen för persondataskyddet och de frågor som aktualiseras inom integritetsskyddsområdet ur olika aspekter inom organisationen.

Rekommendation (10)
Vidareutveckla rutinen för konsekvensbedömningar och säkerställ att rutinen efterlevs i praktiken. Säkerställa att riskanalyser sker kontinuerligt och i enlighet med dokumenterade rutiner.
Åtgärd
Utveckla arbetet kring konsekvensbedömningar i tillägg till den befintliga mallen för konsekvensbedömningar. Införliva riskanalyser och upprättandet av konsekvensbedömningar som en del i informationssäkerhetsarbetet i Ifacts.
Förväntad effekt
Bättre struktur och förståelse för när en konsekvensbedömning ska upprättas. Vidare genereras nyttoeffekter genom vidareutveckling av en samlad hantering av konsekvensbedömningar, i de fall en sådan ska upprättas enligt dataskyddsförordningen, inom ramen för informationssäkerhetsarbetet.

Rekommendation (11)
Utarbeta en dokumenterad rutin som säkerställer regelbunden och ändamålsenlig rapportering av dataskyddsarbetet.
Åtgärd
Ett uppföljningsverktyg som går att jämställa med ett årshjul för att följa upp dataskyddsarbetet. Möjligheten att följa upp området som en integrerad del av uppföljningen och rapportering av informationssäkerhetsarbetet utreds.
Förväntad effekt
En bättre överblick av utvecklingen av de olika områdena inom dataskyddsarbetet och synliggörande av integritetsskyddsfrågorna på ledningsnivå.

Rekommendation (12)
Tillse att DSO-rollen är tydligt definierad och att dess arbetsuppgifter saknar intressekonflikter.

Åtgärd

Genom förtydligad rollbeskrivning ytterligare definiera dataskyddsombudets roll inom ramen för befintliga styrdokument i syfte att motverka risken för intressekonflikter. Även i denna del kommer den utredning som initierats av stadskontoret och som avser resurskartläggning i förhållande till områdena för informationssäkerhet och dataskydd tjäna som grund för att ytterligare stärka och på sikt upprätthålla dataskyddsombudets oberoende ställning i förhållande till den övriga organisationen.

Förväntad effekt

Att det ska framgå tydligare vad dataskyddsombudets roll är i förhållande till övriga uppdrag inom samtliga förvaltningar och staden som helhet samt värna om dataskyddsombudets oberoende ställning som tillsynsfunktion.

Rekommendation (13)

Säkerställa att DSO ges resurser och möjlighet att stötta funktionsstödsnämnden i den utsträckning som behövs.

Åtgärd

Stadskontoret är mitt uppe i en rekryteringsprocess av ytterligare ett dataskyddsombud i syfte att stärka upp de personella resurserna på dataskyddsområdet. Arbetet med denna åtgärd har således redan påbörjats.

Förväntad effekt

Utökade personella resurser som kommer ge förbättrade faktiska möjligheter att ge hela organisationen, inte enbart funktionsstödsnämnden, stöd inom området för dataskydd.

Ordförande

Katrin Stjernfeldt Jammeh

Sekreterare

Belma Rosarv

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