Datum
2022-03-28
Adress

Diarienummer
GYVF-2022-281

Yttrande

Till
Revisorskollegiet

Granskning av dataskyddsarbete (GDPR)
SR-2021-93

Gymnasie- och vuxenutbildningsnämnden beslutar att lämna följande yttrande:

Sammanfattning
Gymnasie- och vuxenutbildningsnämnden redovisar vilka åtgärder som skall vidtas med anledning av de iakttagelser, bedömningar och rekommendationer som gjorts i samband med granskningen av nämndens arbete kring dataskydd. Granskningen har genomförts av EY på uppdrag av stadsrevisionen.

Yttrande
Sammanfattande svar utifrån rapportens slutsats
Revisionen visar att gymnasie- och vuxenutbildningsnämnden delvis men inte i tillräcklig utsträckning bedriver ett systematiskt och ändamålsenligt arbete kring dataskydd. Gymnasie- och vuxenutbildningsnämnden instämmer i rapportens slutsats att nämnden behöver stärka sitt arbete kring dataskydd.

Nämnden kommer att arbeta aktivt med de åtgärdspunkter som lyfts i rapporten. Delar av arbetet har påbörjats och kommer att intensifieras under 2022.

Åtgärder – Kommunstyrelsen och samtliga granskade nämnder

Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen
I samband med att en dataskyddssamordnare anställdes inom gymnasie- och vuxenutbildningsförvaltningen i oktober 2021 påbörjades arbetet med en övergripande granskning av nämndens arbete kring dataskydd. Arbetet ska bland annat resultera i en handlingsplan för granskning och uppföljning på olika aspekter av dataskyddsarbetet. En anvisning kopplas till varje granskningsområde så att granskningen utförs på ett enhetligt sätt i alla verksamheter.

Tidsatta och väl definierade aktiviteter i en handlingsplan gör det också enklare att visa på framsteg och utveckling av dataskyddsarbetet.

Senast genomfört: handlingsplan framtagen maj 2022

Förväntade effekter: Handlingsplanen för granskning hjälper till att synliggöra, förankra och utveckla arbetet kring dataskydd i nämndens samtliga verksamheter. Den möjliggör skapandet av en levande dataskyddskultur, ger struktur och viss förutsägbarhet i det löpande arbetet, samt utgör underlag för uppföljning. Nämnden kommer på ett mer systematiskt sätt kunna följa att nämnden lever upp till dataskyddsförordningens ansvarsskyldighet kring de grundläggande principerna om personuppgiftsbehandling.

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

Nämnden ser över resurs- och ansvarsfördelningen kopplat till informationssäkerhets- och dataskyddsområdet, där identifiering av vilken kompetens som behövs är en central del.

Revisionsrapporten beskriver att det finns en otydlig rollfördelning mellan dataskyddsombud och nämnderna. Det finns ett behov av att förtydliga vissa stadsgemensamma styrdokument, både ur innehålls- och rollfördelningsperspektiv, vilket är stadskontorets ansvar. Nämnden kommer oaktat detta att kunna driva det egna förbättringsarbetet och säkerställa att den interna ansvarsfördelningen är tydlig.

Nämnden har identifierat ett behov av att förtydliga ansvar i de fall systemförvaltningen bedrivs av en annan nämnd. Ett arbete med övriga utbildningsförvaltningar för att se över process och ansvarsfördelningen kring hantering av personuppgiftsincidenter för gemensamma system har påbörjats.

Senast genomfört: Q3 2022

Förväntade effekter: På sikt ett mer proaktivt och självgående arbete kring dataskydd i förvaltningens samtliga verksamheter vilket möjliggörs genom att ansvar för olika delar av dataskyddsarbetet blir tydligt för alla.

Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data. Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.

Del 1 – Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data.
Rutinen för klassificering av informationstillgångar ägs och förvaltas idag av stadskontorets informationssäkerhetssamordnare och ansvaret för att utveckla rutinen utifrån granskningens resultat ligger hos stadskontoret.

Nämnden kommer att säkerställa att det sker en identifiering och klassificering som omfattar även ostrukturerad data. Ett viktigt arbete i samband med detta är att gå från ostrukturerad till strukturerad information så långt som möjligt.

Senast genomförd: Q4 2022

Förväntad effekt: Ökad följsamhet mot dataskyddsförordningen genom bättre kontroll över ostrukturerad data.

Del 2 – Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.
För närvarande genomförs en granskning och uppdatering av nämndens registerförteckning som därefter ska överföras från Excel-filer till iFacts, som är Malmö stads gemensamma IT-stöd för informations- och systemsäkerhet. I samband med överföringen granskas personuppgiftsbehandlingarna, som utgör registerförteckningen, för att säkerställa riktighet. Förväntningarna är att övergången till iFacts ska underlätta den löpande uppföljningen. En rutin som säkerställer att arbetet med registerförteckningen hålls levande kommer att tas fram i anslutning till detta arbete.

Senast genomfört: maj 2022

Förväntade effekter: En samlad och komplett bild över nämndens personuppgiftsbehandlingar som hålls aktuell över tid. En ökad följsamhet mot dataskyddsförordningen och tillvaratagande av de registrerades rättigheter.

Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för
Ändamål för personuppgiftsbehandlingar ska specificeras i registerförteckningen. Den rutin som efterfrågas är en del av rutinen för registerförteckningens riktighet och fullständighet och åtgärdspunkten är således besvarad ovan under rubriken ”*Del 2 – Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid*”.

Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid
En rutin och en mall som kan användas för att följa upp nämndens biträden och leverantörer inom området för dataskydd kommer att tas fram och blir en del av handlingsplanen för granskning och uppföljning. Därutöver sker riktade kontroller eller uppföljning av avtal vid behov.

I samband med det påbörjade arbetet med granskning av nämndens registerförteckning sker en kontroll av att det finns personuppgiftsbiträdesavtal (PUB-avtal) samt instruktioner för hur biträdet (leverantören) ska behandla nämndens personuppgifter.

Senast genomfört: införd i handlingsplan maj 2022

Förväntade effekter: Genom en kontinuerlig översyn av personuppgiftsbiträden och leverantörers åtaganden säkerställs kontrollen över personuppgiftsbehandlingen samt aktualiserar frågor kring nya och förbättrade skyddsåtgärder.

Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken
Incidenthantering sträcker sig från att upptäcka en personuppgiftsincident till att den rapporteras, analyseras, registreras och eventuellt anmäls till Integritetsskyddsmyndigheten. Nämnden kommer säkerställa att alla anställda har information om vad en incident är ur ett dataskyddsperspektiv och hur den ska hanteras. Det pågår ett arbete med att ta fram ett introduktionsprogram för nyanställda, där information om dataskydd och personuppgiftsincidenter blir en del. Rutinerna för incidenthantering kommer att ses över för att säkerställa att de är ändamålsenliga.

Personuppgiftsincidenter kan också rapporteras av någon av nämndens leverantörer av IT-system. I samband med översynen av PUB-avtal och tillhörande instruktioner kontrolleras det att nämnden har utsedda kontaktpersoner för externa parter.

Ett arbete har påbörjats med att kartlägga processen för incidenthantering i de fall nämnden har system som delas mellan de olika utbildningsnämnderna. Syftet är att ta fram en gemensam riktlinje som fastställer kontakt- och eskaleringsvägar samt ansvar för rapportering och information till drabbade.

Uppföljning av hur incidenthanteringsrutinen efterlevs blir en aktivitet i handlingsplanen för granskning och uppföljning.

Senast genomfört: rutinen genomgången och aktivitet för uppföljning införd i handlingsplanmaj 2022. Övriga insatser ska vara genomförda Q4 2022.

Förväntade effekter: Alla i verksamheten känner till när och hur man rapporterar en personuppgiftsincident. En ökad medvetenhet leder till att antalet inrapporterade incidenter ökar. Arbetet med incidenter kan visa på brister som föranleder ett förbättringsarbete.

Åtgärder – gymnasie- och vuxenutbildningsnämnden

Nedan följer åtgärdspunkter särskilt riktade till gymnasie- och vuxenutbildningsnämnden.

Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid
Denna åtgärdspunkt är delvis besvarad under rubriken ”*Del 2 – Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid*” ovan.

Förutom att säkerställa att befintliga personuppgiftsbehandlingar hålls uppdaterade i registerförteckningen behöver nya behandlingar registreras för att förteckningen ska vara komplett. En rutin kommer att tas fram som säkerställer att detta görs i samband med att en behandling startar. Uppföljning av registerförteckningen kommer att bli en del av handlingsplanen för granskning och uppföljning av dataskyddsarbetet.

Senast genomfört: uppföljning infört i handlingsplan maj 2022.
Rutin framtagen maj 2022.

Förväntade effekter: En komplett registerförteckning vilket medför att nämnden får kontroll över samtliga sina personuppgiftsbehandlingar.

Utarbeta en rutin som säkerställer att centralt framtagna styrdokument anpassas utefter den egna verksamheten
Nämnden har gjort ett fåtal anpassningar av de stadsgemensamma styrdokumenten men avser att fortsätta och intensifiera det arbetet. En förteckning över styrande dokument tas fram för att kunna ha kontroll över dokumenthanteringen inom dataskyddsområdet.

Senast genomfört: Förteckning klar i april 2022

Förväntade effekter: Relevanta och uppdaterade styrdokument

Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin
Rutinen för informationsklassning och riskanalys är gemensam för samtliga förvaltningar och har tagits fram av informationssäkerhetsansvarig inom Malmö Stad. Det finns riktlinjer att följa för både riskanalys och konsekvensbedömning men det krävs information och utbildning inom området för att få till ett strukturerat arbete.

En översyn av genomförda riskanalyser och en inventering av ej genomförda riskanalyser ska införas i handlingsplanen för granskning och uppföljning.

Senast genomfört: införd i handlingsplan maj 2022.

Förväntade effekter: Riskanalyser och konsekvensbedömningar genomförs strukturerat vilket medför att personuppgifters skyddsbehov identifieras och att personuppgifter förses med adekvata skyddsåtgärder.

Säkerställa att det finns tillräckliga resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen
För att säkerställa att det finns tillräckliga resurser för ett ändamålsenligt arbete ser nämnden för närvarande över den interna ansvarsfördelningen och vilken kompetens som krävs för de olika delarna i dataskydds- och informationssäkerhetsarbetet. Nämnden kommer via

genomförandet av andra åtgärdspunkter i rapporten och kompetensöversynen få en bättre överblick av vilken kompetens och vilka resurser som behövs inom olika delar av verksamheten.

Senast genomfört: Q3 2022

Förväntade effekter: Tydlig ansvarsfördelning, rätt kompetens och adekvata resurser för att utföra ett ändamålsenligt dataskyddsarbete.

Ta fram en rutin för att säkerställa att gallring av personuppgiftsbehandlingar utförs enligt definierad process

Nämnden har en framtagen arkivredovisning som är avsedd att fungera som ett stöd vid bland annat gallring. Kontroll av hur gallring genomförs i praktiken kommer att ingå som en del av handlingsplanen för granskning och uppföljning av dataskyddsarbetet.

Senast genomfört: infört i handlingsplan maj 2022

Förväntade effekter: Större följsamhet mot dataskyddsförordningens grundläggande principer om lagringsminimering.

Utarbeta en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i gymnasie- och vuxenutbildningsnämndens IT-system

En översyn, och vid behov revidering, av befintliga rutiner för behörighetskontroll i nämndens centrala IT-system genomförs.

Senast genomfört: maj 2022.

Förväntade effekter: Ökat skydd för personuppgifter genom att endast anställda med ett uttalat uppdrag att hantera dessa har åtkomst i systemen.

Ta fram och dokumentera en rutin för att säkerställa att tillräcklig information loggas i samband med incidentrapportering

Befintliga rutiner kommer att kompletteras och förtydligas för att säkerställa att de registrerades rättigheter upprätthålls, bland annat vad gäller hur och vem som informerar den/de drabbade i samband med en personuppgiftsincident.

Senast genomfört: maj 2022

Förväntade effekter: Större följsamhet mot dataskyddsförordningen vad gäller hantering av personuppgiftsincidenter.

Ordförande

Juan-Tadeo Espitia

Förvaltningsdirektör

Anneli Schwartz

Särskilt yttrande från Centerpartiet och Moderaterna.
Särskilt yttrande från Sverigedemokraterna.