Datum
2022-12-02

Tjänsteskrivelse

Vår referens
Björn Westerfors
Förvaltningsjurist
bjorn.westerfors@malmo.se

Granskning av dataskyddsarbete (GDPR)
GYVF-2022-281

Sammanfattning
Malmö stadsrevision har i slutet på 2021 granskat gymnasie- och vuxenutbildningsnämndens efterlevnad av EU:s dataskyddsförordning (GDPR). Syftet med granskningen var att bedöma om nämnden säkerställer ett ändamålsenligt dataskyddsarbete. I granskningsrapporten var den samlade bedömningen att nämnden inte i tillräcklig utsträckning har säkerställt att dataskyddsarbetet bedrivs ändamålsenligt.

Revisorskollegiet behandlade rapporten under januari 2021 och rapporten skickades till nämnden för yttrande. Yttrandet var avsett att ge svar på vilka åtgärder nämnden skulle vidta med anledning av de bedömningar och rekommendationer som redovisades i rapporten. Det framgick även när åtgärderna senast ska vara genomförda.

Nämnden yttrade sig i mars 2022 med förslag på hantering av de åtgärdspunkter som lyfts i rapporten. Nämnden har under 2022 stärkt sitt arbete med dataskydd och informationssäkerhet.

Förvaltningen har tagit fram ett förslag till uppföljande yttrande att översända till revisorskollegiet.

Förslag till beslut
Gymnasie- och vuxenutbildningsnämnden föreslås besluta att godkänna förvaltningens förslag till yttrande och översända yttrandet till revisorskollegiet.

Beslutsunderlag
- Mall för yttrande över granskning av dataskyddsarbete
- Missiv om granskning av dataskyddsarbete (GDPR)
- Rapport om granskning av efterlevnad av dataskyddsförordningen (GDPR)
- Beslut GVN 2022-03-25 §41 Granskning av dataskyddsarbete (GDPR)
- Yttrande till revisorskollegiet - granskning av dataskyddsarbete
- G-Tjänsteskrivelse GVN-2022-12-16 Uppföljande yttrande över granskning av dataskyddsarbetet (GDPR)
- Förslag till uppföljande yttrande över granskning av dataskyddsarbete (GDPR)

Beslutsplanering
Gymnasie- och vuxenutbildningsnämndens arbetsutskott 2022-03-16
Gymnasie- och vuxenutbildningsnämnden 2022-03-25
Gymnasie- och vuxenutbildningsnämndens arbetsutskott 2022-12-06
Gymnasie- och vuxenutbildningsnämnden 2022-12-16

Beslutet skickas till
Revisorskollegiet

Ärendet

Bakgrund
Malmö stadsrevision har i slutet av 2021 granskat gymnasie- och vuxenutbildningsnämndens efterlevnad av EU:s dataskyddsförordning (GDPR). Granskningen omfattade även kommunstyrelsen, servicenämnden och funktionsstödsnämnden och har genomförts av revisionsbyrån EY. Syftet med granskningen var att bedöma om kommunstyrelsen och de granskade nämnderna säkerställer ett ändamålsenligt dataskyddsarbete. Granskningen sammanställdes i en granskningsrapport.

Av rapporten framgår att den samlade bedömningen är att kommunstyrelsen och 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. Det saknas tillräckliga kontroller, uppföljning och rapportering av dataskyddsarbetet. Utbildningsinsatserna är otillräckliga och det saknas ett systematiskt arbete som säkerställer en god kunskapsnivå avseende dataskydd och informationssäkerhet.

Rapporten visar även på att det finns en övergripande organisation och arbetsgång med tillhörande roller samt rutiner för risk- och sårbarhetsanalyser och riktlinjer för personuppgiftsincidenter men att det råder oklarheter mellan kommunstyrelsen och nämnderna vad avser ansvaret för dataskyddsarbetet.

I EY:s granskningsmetod bedöms en organisations mognadsgrad vad gäller dataskyddsarbete. Enligt den metoden framkommer att kommunstyrelsen och de granskade nämnderna har en låg mognadsgrad sett till kommunens storlek, riskbild samt den mängd personuppgifter som hanteras. På en femgradig skala har EY lämnat följande mognadsbedömningar:

- Kommunstyrelsen 2,61
- Servicenämnden 2,47
- Gymnasie- och vuxenutbildningsnämnden 2,42
- Funktionsstödsnämnden 2,47

Rapporten lämnar ett antal rekommendationer till kommunstyrelsen och de granskade nämnderna. Rekommendationerna är uppdelade utifrån angelägenhet i rekommendationer som inledningsvis bör åtgärdas och rekommendation som därefter bör åtgärdas. Rekommendationerna är även uppdelade utifrån rekommendationer som är gemensamma för kommunstyrelsen och de granskade nämnderna samt rekommendationer per granskad nämnd.

Rekommendationerna som rör gymnasie- och vuxenutbildningsnämnden är följande:

Kommunstyrelsen och samtliga granskade nämnder rekommenderas att:

Inledningsvis:

- Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen.
- Tillse att ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.

Därefter:

- Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerade data. Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.
- Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.
- Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.
- Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.

Gymnasie- och vuxenutbildningsnämnden rekommenderas att:

Inledningsvis:

- Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid.
- Utarbeta en rutin som säkerställer att centralt framtagna styrdokument anpassas utefter den egna verksamheten.
- Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.
- Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.

Därefter:

- Ta fram en rutin för att säkerställa att gallring av personuppgiftsbehandlingar utförs enligt definierad process.
- Utarbeta en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i gymnasie- och vuxenutbildningsnämndens IT-system.
- Ta fram och dokumentera en rutin för att säkerställa att tillräcklig information loggas i samband med incidentrapportering.

Revisorskollegiet behandlade rapporten vid sitt sammanträde 2022-01-26 och beslutade att överlämna rapporten till nämnden för yttrande. Yttrandet skulle ge svar på vilka åtgärder nämnden avser att vidta med anledning av de bedömningar och rekommendationer som redovisas i rapporten. Det skulle även framgå när åtgärderna senast ska vara genomförda.

Nämnden yttrade sig i mars 2022 med förslag på hantering av de åtgärdspunkter som lyfts i rapporten. Nämnden har under 2022 stärkt sitt arbete med dataskydd och informationssäkerhet. Av det uppföljande yttrandet framgår mera utförligt de åtgärder som vidtagits, vad som återstår och när de senast ska vara genomförda.

Ansvariga
Emma Sandberg Ekonomichef