Utbildnings- och arbetslivsförvaltningen
Handläggare Malin Karlsson,
verksamhetsutvecklare/nämndsekreterare

Mottagare
Barn- och utbildningsnämnden

Uppföljning av dataskyddsombudets granskning av molntjänster

Förlag till beslut
Informationen tas emot.

Sammanfattning
Dataskyddsombudet har genomfört en granskning av nämndens hantering av personuppgifter i molntjänster så som Microsoft Office 365 (O365), och har presenterat förslag till åtgärder. Förvaltningen har identifierat specifika åtgärder för att säkra behandlingen av personuppgifter i O365, inklusive att kontrollera kryptering och specificera vilka tjänster och data som ska omfattas. Det har även framkommit att Regionstyrelsen ännu inte har etablerat riktlinjer för arbete med molntjänster.

För att säkerställa hantering av personuppgiftsbehandlingar i molntjänster, har förvaltningen implementerat rutiner och en lista på intranätet (Insidan) med godkända och icke godkända digitala verktyg. Listan är till för att göra det enklare för medarbetare att veta vilka digitala verktyg de kan och inte kan använda.

För att möta kraven på tillsyn och revision arbetar förvaltningen med att implementera objektförvaltarmodellen som är ett systematiskt arbetssätt att arbeta med uppföljning av våra system. Sammantaget indikerar bedömningen att förvaltningen har en positiv dialog med dataskyddsombudet och är engagerad i att åtgärda de identifierade bristerna

Ärendebeskrivning
Dataskyddsombudet har som roll att säkerställa att organisationen behandlar personuppgifter enligt rådande lagstiftning. I denna granskning har dataskyddsombudet granskat efterlevnaden av molntjänster inom förvaltningen.

Granskningen visar att nämndens behandlingar av personuppgifter i molntjänster i stort uppfyller kraven på lämplig säkerhet, och att den administrativa säkerheten har förbättrats jämfört med tidigare undersökningstillfälle.

Dataskyddsombudet har lämnat förslag på åtgärder för nämnden.

Regionstyrelsen ansvarar för att säkra det övergripande arbetet inom Region Gotland.

Dataskyddsombudets förslag till nämnden

1. Ta aktiv ställning till om användning av molntjänster som Microsoft Office 365 (O365) är lämpliga för behandling av större mängder av eller känsliga personuppgifter utifrån samtliga aktörer som behandlar eller får tillgång till uppgifterna.

   Svar från förvaltningen:
   Förvaltningen har tillsammans med dataskyddsombudet kommit fram till ett antal åtgärder som förvaltningen behöver göra för att säkra hanteringen av personuppgifter i O365. Det handlar om att kontrollera hur vi krypterar våra uppgifter, vilka tjänster som behöver kryptering och vilka uppgifter vi sparar i O365.

2. Etablera tydliga riktlinjer för uppföljning av molntjänster och molntjänstleverantörer

   Svar från förvaltningen:
   Regionstyrelsen har inte upprättat några riktlinjer kring hur förvaltningarna ska arbeta med molntjänster. Regionstyrelseförvaltningen arbetar med att ta fram rekommendationer för regionen men ärendet har ännu inte kommit till beslut i Regionstyrelsen.

   Fram tills dess att riktlinjer finns på plats arbetar förvaltningen aktivt med att säkerställa att de molntjänster som används följer de lagar som gäller. Förvaltningen följer även eventuell information och uppdateringar som kommer från den Europeiska dataskyddsstyrelsen och Integritetsskyddsmyndigheten (IMY) i Sverige.

3. Säkerställa att behandlingar av personuppgifter i molntjänster är dokumenterade så att de kan förvaltas och följas upp.

   Svar från förvaltningen:
   Förvaltningen har idag en rutin för alla anställda som vill införskaffa ett digitalt verktyg, som en app, en websida eller ett system. Enklare digitala verktyg som inte innehåller några personuppgifter och de tjänster där nämnden har tecknat ett personuppgiftsbiträdesavtal finns registrerade i en lista, som har döpts till "Gröna Listan".

   För att kunna efterleva de krav som ställs vid innehav av ett system, till exempel säkerhetsklassning och förvaltningsplan med budget, finns förvaltningens system registrerade i LISa. (ledningssystem för informationssäkerhet)

   Förvaltningens rutin innebär att ett digitalt verktyg inte får användas förrän GDPR har säkrats och personuppgiftsbiträdesavtal har tecknats.

4. Se över vilka uppgifter nämnderna behandlar i Adobe, Hypergene, Icloud och Visma samt se till att de är korrekt klassade och införda i LISa utifrån de uppgifter nämnderna behandlar

   Svar från förvaltningen
   iCloud används idag på gymnasiet och vuxenutbildningen då de har Macdatorer. Dock är rekommendationen från förvaltningen att dokument ska sparas i O365. Arbete med denna fråga pågår inom förvaltningen. Regionstyrelsen är ägare av Adobe, Hypergene och Visma, vilket innebär att ansvar för att systemen är rätt klassade i LISa ligger på regionstyrelsen.

5. Inför och dokumentera de konkreta tillsynsåtgärder som ska genomföras som en del av förvaltningen, se nedan exempel på åtgärder Riktlinje för hur ofta loggar ska samlas in och granskas beroende på uppgifternas känslighet

   1. Insamling av uppgifter om utförarna genomfört egna säkerhetsrevisioner i sin egen och sina underleverantörers verksamhet
   2. Insamling och granskning av incidenter i utförarens verksamhet
   3. Stickprovskontroll av hur en begäran om rättelse, radering eller begränsning av behandling utförs
   4. Revision av att behandling sker i enlighet med den instruktion som Region Gotland lämnat
   5. Kontrollera att biträdets personal som får tillgång till uppgifterna har skrivit på och fått tydlig instruktion om att arbetsuppgifterna omfattas av rättslig förpliktelse avseende sekretess

   Svar från förvaltningen:
   Punkt 1. Förvaltningen kommer att arbeta efter objektförvaltarmodellen under år 2024. Det medför att vi kommer gå igenom våra avtal för att se vad som är överenskommet med våra leverantörer. Se punkt 4.

   Punkt 2. Förvaltningen har en bra och tydlig rutin för hur personuppgiftsincidenter ska hanteras. Förvaltningen behöver dock utveckla arbetet för att bli bättre på att upptäcka och anmäla dessa. När det gäller it - incidenter har förvaltningen ingen rutin. Det är inbokat en utbildning med Regionstyrelsen i hur förvaltningen ska hantera dessa incidenter i den process som finns.

   Punkt 3 hanteras genom att kontaktpersonen för GDPR på förvaltningen har begärt registerutdrag på sig själv. När det gäller rättelse och radering inkommer det väldigt få per år och dessa är oftast felinskickade och ska inte hanteras utifrån GDPR

   Punkt 4 - 5 hanteras i Region Gotlands objektsförvaltningsmodell där de som förvaltar ett system årligen ska göra en förvaltningsplan. I den planen ska uppföljning av leverantören ingå.

Bedömning

Förvaltningen har en bra dialog med dataskyddsombudet och arbetar med att åtgärda de rekommendationer som ombudet har inkommit med. Dock är det några punkter där förvaltningen är beroende av att Regionstyrelsen genomför vissa ändringar. Där inväntar ännu förvaltningen en plan för hur dessa ska genomföras.

Beslutsunderlag

Förvaltningens tjänsteskrivelse, 2024-02-14
Rapport uppföljning av UAF molntjänster

Utbildnings- och arbetslivsförvaltningen

Torsten Flemming
Utbildningsdirektör

Bo Eriksson
Avdelningschef stöd och utveckling

Skickas till

Dataskyddsombudet