RAPPORT

2023 år uppföljning av 2021 års inventering och problem med användning av molntjänster enligt den Europeiska Dataskyddsförordningen (GDPR)

Fastställd av Barn- och ungdomsnämnden
Framtagen av Regionens dataskyddsombud
Datum 20231026
Gäller
Ärendenr BUN 2023/3000
Version 1

Barn- och ungdomsnämnden
Region Gotland

Uppföljning inventering och problem med användning av molntjänster inom Barn- och ungdomsnämnden 2023

Innehåll

SAMMANFATTNING

Nämndens behandlingar av personuppgifter i molntjänster uppfyller i stort kraven på lämplig säkerhet, och den administrativa säkerheten har förbättrats jämfört med tidigare undersökningstillfälle. Problemet med det oklara rättsläget avseende Office 365 kvarstår dock, även om förutsättningarna förbättrats genom EU's adekvansbeslut och Microsofts initiativ att utforma tjänsten för att följa de regulatoriska kraven.

Förslag på åtgärder:

I huvuddrag kan förslagen sammanfattas i tre punkter som i allt väsentligt gäller samtliga nämnder.

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

2 Etablera tydliga riktlinjer för uppföljning av molntjänster och molntjänstleverantörer

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

Den tjänster som bedömdes som mest angelägen att utvärdera och ta ställning till var

och är användningen av Office 365. Användningen av sociala medier bör kontrolleras särskilt när behandlingen avser skolpliktiga elevers personuppgifter.

Nämnden bör undersöka och vid behov åtgärda om särskilt skyddsvärda personuppgifter förekommer i fakturor som behandlas i Visma.

I och med att användningen av molntjänster generellt ökar som en konsekvens av att leverantörerna i allt högre grad går över till den leveransmodellen för sina tjänster, är det av fördel att nämnden tar ställning till i vilka fall det är lämpligt för att kunna samordna med andra nämnder med liknande behov. Ett exempel på det är Microsoft 365 som sedan det sedan en tid diskuterats ett bredare införande av i nämnderna.

Frågan om lämpligheten att använda USA-kontrollerade tjänster har fått ny aktualitet genom det adekvansbeslut som EU-kommissionen fattat, men det råder inte samsyn kring hur det ska tolkas. Att användningen av IT-tjänster i allt högre utsträckning går över mot molntjänster innebär ett potentiellt problem, då leverantörerna i många fall inte beaktar eller ens känner till de regulatoriska krav som offentlig sektor har att förhålla sig till. Kraven på molntjänsterna och deras huvudmän gäller även deras underleverantörer, vilket gör att alla som deltar i behandlingen måste uppfylla kraven som ställs på tjänsten. Effekten blir att regionen måste vara vaksam på och vara tydlig med kravställning och uppföljning av att tjänsterna är lämpliga för verksamheten och på ett effektivt sätt skyddar de registrerades integritet. Även förvaltningen av molntjänster behöver därför utvecklas i linje med förslagen i skrivelse RS 2022/1850.

BAKGRUND

Dataskyddsombudet genomförde en granskning av användningen av molntjänster 2021 [RS 2021/1647], i rapporten identifierades brister i hanteringen. Denna undersökning avser att följa upp om problem som då identifierades har lösts eller kvarstår samt uppdatera förekomsten av molntjänster som används inom förvaltningarna.

Regionen har ett etablerat arbete med informationssäkerhet och skydd för personuppgifter. Det finns en införd LIS där informationsmängder klassas utifrån informationssäkerhet. Att det är informationsmängder som klassas gör att det inte är behandlingar av informationen som klassas vilket förenklar när informationsmängd specifika system och arbetsprocesser är entydiga, men försvårare att hitta information om behandlingar som omfattar flera system eller behandlar olika uppgifter. Utifrån GDPR's krav är det även en brist att det inte primärt är de behandlingar som görs med personuppgifterna som dokumenteras.

Aktuella risker och problem med molntjänster

Molntjänster skiljer sig mot andra leveransmodeller för IT genom att de är leverantören

som har fullständig kontroll över tjänsterna, med begränsade möjligheter för användarna att påverka utformningen och utförandet. Då personuppgiftsansvariga är skyldiga att säkerställa att behandlingen sker med lämplig teknisk och administrativ säkerhet, behöver det finnas en dokumenterad riskbedömning av de tjänster som används. Användningen av molntjänster pekas sedan flera år ut som en av huvudorsakerna bakom informationsincidenter.[1]

Förutom de rena säkerhetsproblemen kan det även föreligga legala problem när tjänsterna inte följer svenska regler. Det förekommer att avtalsvillkor för användning av standardtjänster har villkor som kommer i konflikt med reglerna för offentliga verksamheter. För att det ska fungera behöver det säkerställas att leverantörerna förstår och har förmåga att följa svenska regler vilket inte är begränsat till GDPR utan även omfattar t.ex. sekretess enligt OSL. I och med att uppgifterna lämnas ut till molntjänstleverantörerna anses uppgifterna röjda, med följd att det måste antas uppstå en skada om uppgifterna omfattas av omvänt skaderekvisit. Ett röjande av sådana uppgifter kan medföra straffansvar enligt BrB 20 kap. 3 § för den som fattar beslut om utlämnande. Genom införandet av den nya bestämmelsen i OSL 10 kap. 2 a § med en ny sekretessbrytande grund vid utkontraktering av lagring och bearbetning av information, har dessa problem i viss grad undanröjts. Det krävs dock att ett röjande i en sådan situation inte är olämpligt, varför lämplighetsprövning fortfarande måste göras innan uppgifterna lämnas ut.

Även om det kan visa sig juridiskt möjligt att utkontraktera tjänsten och informationshanteringen, så kan det vara olämpligt ur ett säkerhetsperspektiv[2], vilket understryker vikten av att genomföra och dokumentera ett sådant beslut.

Molntjänster kan även ha komplexa beroenden till ett flertal underleverantörer vilket gör att inte bara kontraktspartnern för en molntjänst måste studeras, utan även övriga parter som på något sätt behandlar eller har åtkomst till uppgifterna. Vid upphandling är det därför viktigt att kraven på efterlevnad av GDPR, OSL och andra tillämpliga författningar även ska omfatta alla underleverantörer som behandlar eller får del av personuppgifterna.

Den huvudsakliga kontrollen sker genom den avtalsreglering som finns av tjänsten, vilket gör att det är viktigt att förstå avtalsregleringens innebörd i förhållande till tjänstens utformning och att det är möjligt för såväl den personuppgiftsansvarige och de registrerade att hävda sina rättigheter. Avtalsvillkor som föreskriver prövning av avtalsvillkoren av domstolar i andra länder t.ex. USA kan generellt inte anses uppfylla de kravet.

Uppföljning av behandlingen i molntjänsterna

[1] Cost of a Data Breach Report 2023 IBM/Ponemon Group
[2] E-sam Adekvansbeslut och ny sekretessbrytande bestämmelse– grönt ljus för amerikanska molntjänster? 20230609

Ett område som generellt är svårt och inte får den uppmärksamhet det försenar är uppföljning av hur krav på behandlingar och processer kring dem efterföljs. Det framgår av SKR's mall för PUB-avtal (*9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.)*
När behandlingen utförs av en molntjänstleverantör lokaliserad långt från den personuppgiftsansvarige, blir uppföljning typiskt sett svårare att genomföra, vilket måste beaktas i de riskanalyser som görs för behandlingen. Att förlita sig helt på egenkontroller kommer sannolikt inte att accepteras när behandling omfattar särskilt skyddsvärda uppgifter.
Då biträdet ska genomföra egenkontroll är det lämpligt att personuppgiftsansvariga begär in och tar del av resultatet av egenkontrollen och då det finns anledning eller som stickprov ställer fördjupande frågor till biträdet och eventuella underbiträden. Förslagsvis kan detta föras in som en del av systemförvaltningsprocessen.

Tjänster baserade i USA eller utanför EU/EES i övrigt

Då många av de populära molntjänster som används är lokaliserade i USA uppkom efter EU-domstolens utslag i Schrems II målet frågan om de kan användas utan att bryta mot GDPR. Domen tog framför allt fasta på de rättsliga förutsättningar som gäller för företag som omfattas av USA's (The Foreign Intelligence Surveillance Act of 1978 (FISA) lagstiftning.

Den 10 juli 2023 presenterade EU ett adekvansbeslut avseende EU-U.S. DPF Principles, inklusive Supplemental Principles och Annex I som i princip slår fast att det inte föreligger ett legalt hinder för överföring av personuppgifter till USA förutsatt att leverantören lever upp till övriga säkerhetskrav och genomfört ITA's självcertifiering. Huruvida det nya beslutet kommer att överleva en prövning av EU-domstolen är dock oklart i och med att flera av de principiella invändningarna rörande möjligheten för USA's myndigheter att få del av uppgifter sannolikt inte förändrats på ett avgörande sätt. De registrerades rättigheter som nu uppges vara lösta genom USA's utfärdande av Executive Order 14086 som inför kontrollmekanismer i syfte att stärka skyddet för den personliga integriteten står fortfarande mot övervägande om nationell säkerhet. Till dess att det föreligger en domstolsprövning från EU-domstolen (troligen inom 2-3 år) som antingen fastställer eller undanröjer adekvansbeslutet är det därför formellt möjligt att använda lösningar från USA baserade leverantörer, t.ex. Microsoft 365 under förutsättning att lösningen bedöms ha en lämplig säkerhet för de uppgifter som ska behandlas.

Givet att lagligheten sannolikt kommer att ifrågasättas på nytt och de svårigheter som föreligger i att visa att skyddsmekanismerna för EU-medborgares integritet kommer att vara tillräckliga när de kommer i konflikt med USA's säkerhetsintressen, bör det dock även fortsatt göras en riskprövning vid användning av dessa tjänster innan det beslutas om användande inte minst för att undvika överträdelser av sekretessen i OSL. Även om

behandlingen är formellt inte är olaglig innebär det inte med nödvändighet att den är lämplig, vilket kommer då även kommer i konflikt med GDPR.

Oaktat hur den rättsliga situationen utvecklas finns dock krav på att de ansvariga utifrån skyddsvärdet för behandlade uppgifter, bedömer att skyddet är lämpligt i de tjänster som används. Den Europeiska Dataskyddsstyrelsen EDPB har tagit fram rekommendationer
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
som i princip konstaterar att det är den personuppgiftsansvariges ansvar att säkerställa att behandlingen lever upp till kraven som dessutom genomgår evolutionär förändring beroende på juridisk praxis, teknisk utveckling och social adekvans.

Som tidigare nämnts finns anledning att beakta även annan lagstiftning än GDPR avseende skydd för personuppgifter. OSL's regler om sekretess med omvänt skaderekvisit, som avser t.ex. uppgifter inom hälso- och sjukvård, socialtjänst samt viss personaladministration, gör därför att molntjänster från andra länder än Sverige inte bör användas såvida inte skyddsåtgärder som kryptering eller pseudonymisering kan användas eller det tydligt kan visas att sekretessfrågan kan hanteras utan att exponera de ansvariga för personligt straffansvar.

När en molntjänstleverantör tar emot och behandlar uppgifter kommer uppgifterna att röjas varför det måste ske till en utförare som är behörig eller verkar med stöd av lag. Det stödet har införts i lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Även de nya reglerna i OSL 10 kap 2a avseende möjligheten att lämna ut uppgifter med sekretess förutsätter att det sker en lämplighetsprövning. Att enbart avtalsreglera sekretessansvaret om det inte finns ett straffsanktionerat skydd för sekretess i utlandet anses inte vara tillräckligt. För uppgifter som omfattas av sekretess med omvänt skaderekvisit är det därför i regel olämpligt att använda molntjänster där någon del av behandlingen sker utanför Sverige.

Fördelarna med att använda en molnlösning behöver därför i varje situation vägas mot att medborgarna har rätt att förvänta sig att offentlig verksamhet bedrivs med författningsstöd, särskilt om det avser behandlingar som är del av myndighetsutövning mot enskild. Ställningstaganden att använda tjänster behöver därför vara väl underbyggda och kunna motiveras.

I allt väsentligt handlar det om den faktiska kontrollen över uppgifterna och behandlingen av dem. Om en erkänt teknisk säker krypteringslösning används där den personuppgiftsansvarige är den ende som har nyckeln för åtkomst till läsbara uppgifter kan det ifrågasättas om det utifrån GDPR finns risk för obehörig åtkomst eller förvanskning. Det kan dock fortfarande vara problematiskt genom att den personuppgiftsansvarige inte har kontroll över tillgängligheten till uppgifterna och detta har identifierats som viktigt vid informationsklassningen.

Även om det kan visa sig juridiskt möjligt att utkontraktera tjänsten och

informationshanteringen, så kan det vara olämpligt ur ett säkerhetsperspektiv[3], vilket understryker vikten av att genomföra och dokumentera ett sådant beslut.

Microsoft Office 365

Microsoft Office 365 är en så kallad produktivitetsplattform som på grund av komplexiteten i de ingående produkterna (bl.a. Office, Outlook och Teams) och deras integrationer väcker frågor värda en egen utredning. I dagsläget används Office 365 av barn- och utbildningsnämnden samt gymnasie- och vuxenutbildningsnämnden, utrullning har dock stoppats i de övriga förvaltningarna. Det är fortsatt svårt att definitivt uttala sig om Office 365 lämplighet för användas inom kommunal verksamhet, eftersom det dels är beroende av villkor, implementering, behandlade uppgifter och vidtagna skyddsåtgärder. Det har dock under det senaste året skett ett antal förändringar som kan påverka möjligheterna för en bredare användning om det är önskvärt.

1. Microsoft har etablerat tjänsteproduktion inom EU och kan nu sköta behandlingen av uppgifter inom EU
2. Microsoft har etablerat tjänsteproduktion i Sverige vilket gör att de för vissa tjänster sköter hela behandlingen i Sverige.
3. Microsoft uppger att de har gett europeiska partners rätt att bygga upp tjänsteproduktion för Microsofts produkter för att behandling inte ska falla under USA's kontroll
4. Det har införts möjligheter för användarna att använda kryptering där de även kontrollerar krypteringsnycklarna

Sammantaget med EU's adekvansbeslut ökar möjligheten att använda Office 365 betydligt i kommunal verksamhet, givet att en genomgång visar att det är lämpligt för den aktuella verksamheten. Genom att en övergång till Office 365 är en väsentlig förändring av behandlingen och inte är en entydig produkt utan en samling av applikationer och IT-resurser behöver det genomföras en DPIA innan ett eventuellt införande sker. För att kunna landa i att det är lämpligt att använda Office 365, krävs analys och dialog med leverantören. Personuppgiftsansvariga måste förstå och leverantören måste kunna garantera var alla behandlingar, inklusive support och lagring (inklusive backup) sker. Något som troligen kommer att vara möjligt för en del av applikationerna men inte alla, vilket ställer krav på att andra applikationer inte får användas då de är integrerade och byggda för att utbyta information.

Givet att det finns interna administrativa säkerhetsåtgärder (i form av

[3]E-sam Adekvansbeslut och ny sekretessbrytande bestämmelse– grönt ljus för amerikanska molntjänster? 20230609

informationsklassning, behörighetskontroller och loggning), kan det vara möjligt att uppnå en lämplig säkerhet för de registrerade.
En tillkommande dimension är att det kan bli problematiskt att till exempel kommunicera med allmänheten genom Microsofts tjänster om det förutsätter att de måste acceptera Microsofts användarvillkor. Regionen kan inte kräva att allmänheten accepterar villkoren från en utomstående leverantör för att erbjuda en tjänst utan måste i sådana fall erbjuda alternativ, vilket kan vara svårt att hantera effektivt.

RESULTATET AV 2023 ÅRS UNDERSÖKNING

Utbildnings och arberlivsförvaltningens svar

1 Vilka molntjänster som används (länk till tjänsten), om den inte finns med på den bifogade listan

Svar: Utbildnings- och arbetslivsförvaltningen har många olika tjänster som är appar, websidor med mera, vi kallar det för digitala verktyg. De digitala verktygen som inte finns registrerade i systemet LISa, utan på vår Insida. Förvaltningen samlar dessa digitala verktyg i vad vi kallar för gröna listan. I gröna listan delar vi upp de digitala i tre olika kategorier:

Blå: inga personuppgifter behandlas

Grön: Godkänd Pub-avtal finns.
Gul: Godkänd med särskilda förutsättningar
Röd: Underkänd (dvs att det digitala verktyget inte får användas)

För att veta om det digitala verktyget som du önskar använda är uppfyller kraven för GDPR använder du vår e-tjänst. I den ska du besvara några frågor om appen utifrån GPRD. Svaret skickas till vår kontaktperson för GDPR som gör en slutgiltig bedömning.om det digitala verktyget går att använda eller inte.

BUN

Office 365				I förvaltningsplan	?	*under införande och u*	JA
Facebook					Ja	RG bör inte lägga upp personuppgifter eller	JA
Instagram					Ja	RG bör inte lägga upp personuppgifter eller	JA
Forskoleforum.se							JA
Sumab.se							JA
Quizlet.com							JA
sameskolstyrelsen.se		JA				Inga personuppgifter enligt uppgift Oklar avtalssituation	JA
studyalong.se							JA
segotland.speedadmin.dk							JA
Toolify				Nej	Ja via underboträde	Tveksam legal grund för behandlingen hos	JA

2 I vilken del av verksamhet molntjänsten används om det skett en förändring av användningen jämfört med då inventeringen gjordes

Svar: vi har inte gjort några förändringar. Dock ser jag att vi inte har angivit att vi använder Facebook och Instagram. Sen har vi köpt in en ny lärplattform som kommer i drift under sommaren som heter Unikum.

3 Hur ni som personuppgiftsansvariga följer upp användningen av tjänsten

Svar: Gröna listan ska följas upp kontinuerligt dock har detta inte hunnits med. När det gäller våra system så ska det följas upp i enlighet med objektsförvaltarmodellen som håller på att driftsättas. Så vi har ännu inte gjort några uppföljningar. Men under år 2024 ska detta förändras.

4 Vilka åtgärder som vidtagits med anledning av de påtalade problemen i föregående granskningsrapport (detta avser de tjänster som är röd eller gulmarkerade i den bifogade listan.

Svar:

De som var markerade röda:

SchoolSoft slutar vi använda under sommaren.
DigiExam kollar vi upp med tvåfaktorsinlogg. De erbjuder inte det dagsläget.

sameskolstyrelsen.se innehåller inga personuppgifter utan är ett samarbeta för att lära sig samiska på modersmål.
Toolify kommer eller har vi slutat att använda.

De som var markerade gula:

YongLogic (GW) https://www.yonglogic.se/gw-arbetsmarknad/ - håller på att upphandla ett nytt system.

Office 365 – håller på att se över om server i Sverige och kryptering.

Inläsningstjänst: Det innehåller inte några personuppgifter och eleven loggar in via sin e-post. Inläsningstjänst innehåller inlästa läromedel, undervisningsfilmer samt skönlitterära böcker digitalt

De som vi slutat använda:

Pedagog Gotland

Zoom Edu

Genomförda åtgärder med utgångspunkt i identifierade frågor 2021

Dokumentation

Då inventeringen av molntjänster genomfördes 2021 framkom att det inte fanns en heltäckande dokumentation av vilka tjänster som användes. Antalet identifierade tjänster har vid inventeringen 2023 ökat från 13 till 17 identifierade molntjänster, huruvida de nyligen börjat användas eller upptäckts till följd av en ökad medvetenhet är av mindre betydelse. Det väsentliga är att ansvariga har en överblick och kan granska de tjänster som används. För att det ska gå att göra så krävs att de finns dokumentation som personuppgiftsansvariga har åtkomst till och kan följa upp. Det som måste finnas på plats är dokumentation i LiSA vilket det finns för 6 av de identifierade systemen vilket indikerar att dokumentationen över behandlingarna behöver förbättras.

Beslut om användning utifrån klassning

Respektive nämnd har ansvaret för styrningen som annars huvudsakligen sker genom inköpsprocessen

Accepterade avtalsvillkor för molntjänster

Det har inte skett någon central styrning av avtalsvillkor för molntjänster som inte accepteras

Tekniska skyddsåtgärder

I dagsläget har inga RG-kontrollerade tekniska skyddsåtgärder vidtagits.

Riktlinjer för uppföljning av molntjänster

Regionen har tagit fram en objektsförvaltningsmodell som delvis adresserar hur utförandet av molntjänster följs upp

Process för användning av molntjänster

Regionen har uppdaterat sin systeminförandeprocess så att den även omfattar molntjänster

Policy för användning av digitala kommunikationsverktyg

Regionen har inte fattat beslut om vilka verktyg som ska användas, men på intranätet finns en vägledning https://intra.gotland.se/sidor/stod-och-interna-tjanster/it--och-telefoni/tjansteutbud/video--och-webbmotestjanster.html?query=video
som stöd för medarbetare för att välja lämplig kanal.

Personuppgiftsansvarigs uppföljning av behandlingar 2023, ansvarsskyldigheten

Det är väl känt att det är svårt att från centrala funktioner fullt ut kontrollera anskaffningen av molntjänster, speciellt de som inte kräver betalning. I och med att de är lättåtkomliga och enkla att använda utan nedladdning och installation är det dessutom svårt att upptäcka om tjänsterna används. För att säkerställa att reglerna för hantering av personuppgifter följs är det därför viktigt att det sker en aktiv informationsspridning och uppföljning av hur verksamheten hanterar personuppgifter. Om att all användning av molntjänster för behandling av personuppgifter dokumenteras.

Objektförvaltningsmodellen och modellen för systeminförande ger en bra systematik och struktur men är känsligt för att dessa inte är kända eller följs. En förutsättning för att personuppgiftsansvariga har kontroll över behandlingen är att det sker regelbunden uppföljning.

Ett av de viktigaste syftena med GDPR var att personuppgiftsansvariga ska ha kontroll över hur behandlingen sker och säkerställa att den sker med lämplig säkerhet. De måste även säkerställa att de registrerade har möjlighet att utöva sina rättigheter. De

personuppgiftsansvariga måste därför aktivt kontrollera att skyddet är effektivt och att avtalsvillkoren för tjänsterna inte inskränker de registrerades rättigheter. Ett exempel på svårbedömda situationer t.ex. där RG kan anses förvara uppgifter från LinkedIn utan att de är RG som lagt upp dem, och de inte anses ha gjorts allmänt åtkomliga av den registrerade själv genom att de skickat meddelanden till en rekryterare på RG. Det finns därför anledning att vara vaksam med vilka uppgifter som RG efterfrågar och har tillgång till men som inte är allmänt tillgängliga.

GDPR's ansvarsskyldighet gör att ansvaret för att behandlingen följer reglerna och är lämplig faller helt på den personuppgiftsansvarige, med innebörden att utfästelser och garantier från leverantörer har begränsad verkan. Av det skälet är det viktigt att så länge tjänsten används, kontrollera att den administrativa och tekniska säkerheten är lämplig och att reglerna för sekretess följs.

OBSERVATIONER NÄMNDGEMENSAMMA TJÄNSTER

Adobe

Adobe är en tjänst som används av i princip alla förvaltningar och som i de flesta fall är oproblematisk. Det finns dock flera olika tjänster som går under samma beteckning. Den vanligaste är en vanlig pdf-läsare med begränsad funktionalitet som är lokalt installerad och således inte en molntjänst såvida inte extrafunktioner aktiveras. Mer avancerade tjänster för bland annat editering och delning av dokument kan innebära lagring i Adobe's molntjänst, vilket inte är lämpligt för särskilt skyddsvärda personuppgifter som kan förekomma i t.ex. utredningar eller beslut.

Hypergene

Verktyget Hypergene hämtar data från RG's system antingen via filöverföring eller från en utdatabas. Hypergene är behörighetsanpassat på samma sätt som övriga system och det ska inte gå att se mer känslig medarbetardata i Hypergene än i exempelvis HR plus eller Medvind. Sekretessklassade fakturor läses inte in i systemet.
Det kan vara problematiskt med tjänster som hämtar och sammanställer uppgifter ur verksamhetssystemens databaser eftersom det vanligen ger andra kategorier av användare potentiell tillgång till personuppgifter än de som är handläggare av ärendena. Då det införts behörighetskontroll är det viktigt att åtkomsten till uppgifter följs upp och utvärderas för att säkerställa att uppgifterna har ett lämpligt skydd.

Visma (Proceedo)

Fakturahanteringen i molntjänsten Visma Proceedo kan utgöra ett problem när fakturorna innehåller personuppgifter. Problemet ligger i de uppgifter som i vissa fall behövs för faktureringen och som även kan medföra sekretess. Det är inte lämpligt att

använda en molntjänst för sådana uppgifter om det inte kan säkerställas att samtliga biträden som behandlar uppgifterna täcks av lagreglerad sekretess.

DATASKYDDSOMBUDETS BEDÖMNING

Förvaltningen och nämnden har även om de inte anger det vidtagit åtgärder för att adressera de problem som föregående undersökning noterat. Tjänsten Schoolsoft och Toolify är under avveckling och de följer de centralt antagna riktlinjerna för sociala medier. Som ersättare för Schoolsoft införs Unikum som har bättre stöd för att införa lämplig säkerhet. Användningen av Office 365 förenklas av det adekvansbeslut som meddelats men det krävs fortfarande att nämnden bedömer att tjänsten är lämplig för de behandlingar som genomförs med de personuppgifter som behandlas. Det behöver klaras ut om särskilt skyddsvärd information omfattad av sekretess med omvänt skaderekvisit (hälso- och sjukvård, socialtjänst) behandlas i tjänsten, då det sannolikt inte är lämpligt.
Användningen av sociala medier kan vara problematisk speciellt om den används för att behandla personuppgifter om elever som har skolplikt. För att behandlingen inte ska leda till problem behöver användningen vara utformad så att de registrerade fritt väljer att vara med och inte begränsas av att inte välja att godkänna behandling i tjänsterna.

Det är för DSO inte tydligt om samtliga molntjänster som används och finns upptagna i LiSA är med i sammanställningen, ett exempel är Optiplan som används för skolskjuts men som inte finns med i sammanställningen. Enligt uppgift har inte uppföljning av grönmarkerade system skett, men avses ske under 2024, vilket är en förutsättning för kontroll över behandlingarna. Det framhålls att nämnden har en ”grön lista” med molntjänster som bedömts uppfylla kraven, DSO har dock inte lyckats hitta denna på intranätet. Om ”gröna listan” innehåller molntjänster som inte finns upptagna i LISa bör de göra det.

Nämnden behöver ta ställning till vilka uppföljningsåtgärder som är lämpliga att genomföra som en del av förvaltningen, då uppgifter om barn behandlas och det kan befaras att även särskilt skyddsvärda uppgifter behandlas. Även mängden personuppgifter gör att nämnden behöver ställa höga krav på säkerheten och följa upp att behandlingen sker i enlighet med kraven.

Förslag på åtgärder för samtliga nämnder

- Genomför genomgång av de behandlingar där molntjänster används, (detta är även en annan granskningsaktivitet som DSO förordar 2024. Avsikten är att

komplettera LISa med ett register över behandlingar och vilka tjänster som då används.

- Gör en genomlysning av de förutsättningar som finns för respektive nämnd att använda en gemensam MS Office 365 lösning med utgångspunkt i konkreta implementationsscenarier och licenser. (Projekt är enligt uppgift redan startat)
- 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.
- 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
    - Insamling av uppgifter om utförarna genomfört egna säkerhetsrevisioner i sin egen och sina underleverantörers verksamhet
    - Insamling och granskning av incidenter i utförarens verksamhet
    - Stickprovskontroll av hur en begäran om rättelse, radering eller begränsning av behandling utförs
    - Revision av att behandling sker i enlighet med den instruktion som RG lämnat
    - 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

Specifika rekommendationer till Gymnasie-och vuxennämnden

Då nämnden behandlar stora mängder känsliga uppgifter är det särskilt angeläget att etablera en förvaltning som aktivt följer upp leveransen av molntjänster. Det finns därför anledning att etablera en förvaltningsorganisation som har förmåga och kapacitet att följa upp tjänsteleveranserna.