RAPPORT

Uppföljning av Molntjänster inom Region Gotland 2024

För fastställande av Miljö- och byggnämnden
Framtagen av Regionens dataskyddsombud
Datum 20250703
Gäller regionens samtliga nämnder
Ärendenr MBN 2025/1410
Version 1

Miljö- och byggnämnden
Region Gotland

Uppföljning av Molntjänster inom Region Gotland 2024

Innehåll

Sammanfattning

Miljö- och byggnänden följer i allt väsentligt reglerna i GDPR vid användning av molntjänster. De flesta molntjänster som används behandlar inte särskilt skyddsvärda uppgifter men det förekommer behandlingar av personuppgifter om stora mängder användare. Det är dock sannolikt att det kommer att behandlas mer och känsligare uppgifter i molntjänster på grund av marknadsutvecklingen då leverantörerna alltmer övergår till abonnemang och molnleverans.

De frågor som är mest angelägna är om regionens nämnder lever upp till sin ansvarsskyldighet genom att ha kontroll över hur tjänsterna behandlar personuppgifter i montjänsterna, samt om användningen av tjänsterna uppfyller lämplig säkerhet i förhållande till skyddsvärdet för den information som behandlas. Generellt har nämnderna en bättre kontroll och dokumentation av de molntjänster som används jämfört med föregående år. Det har dock utvecklats ett mer generellt ifrågasättande av om behandling av USA-baserade leverantörer är förenligt med GDPR och sekretesslagstiftning. När rapporten skrivs finns det fortfarande inget nytt ställningstagande från EU rörande adekvansbeslutet baserat på Data Privacy Framework som möjliggjort överföringar, men om det förändras kan det få stora konsekvenser för möjligheten att använda många molntjänster.

Det förekommer även annan användning av molntjänster som kan bryta mot GDPR och OSL, t.ex. fakturerings/ ekonomisystemet Proceedo, leverantörskontrollerade applikationer för monitorering inom hälso- och sjukvården. Problemens grund ligger i möjligheten att kontrollera behandlingen och vilka uppgifter som behandlas. Ett sätt att lösa sådana problem illustreras av Assesio Ascend för arbetspsykologiska test där pseudonymisering används som skyddsåtgärd för behandlingar som annars hade varit svåra att genomföra.

Regionens nämnder kommer med införandet av MS365 att behöva se över sina processer för behandling av personuppgifter i molntjänster, vilket med fördel kan leda till generell tillämpning för samtliga molntjänster som används. De områden som är angelägna att se över är kännedom/förståelse av licensvillkoren, behörighetshantering, loggning av åtkomst samt uppföljning av åtkomst till och hur personuppgiftsbehandlingen i tjänsterna sker. Ett ökat beroende av molntjänster måste även balanseras genom att det finns en plan och beredskap för att kunna återta, flytta och/eller producera tjänsterna i egen regi om molntjänsterna inte lever upp till de krav regionens nämnder behöver ställa.

Bakgrund

Under november och december 2024 har uppgifter om regionens användning av molntjänster samlats in från nämnder/förvaltningar. Användningen av molntjänster ökar ytterligare jämfört med tidigare år, och totalt 239 molntjänster har identifierats, för nämnden har det endast tillkommit en molntjänst. Av tjänsterna anges i svaren att totalt 140 är dokumenterade i LISa. Vid sökning i LISa har två ytterligare molntjänster upptäckts. Ett antal (23) av de rapporterade molntjänsterna återfinns inte heller i LISa (219 enligt excelblad), vilket måste betraktas som en stark förbättring jämfört med tidigare år. Att de rapporterade resultaten och de registrerade resultatens skiljer sig åt kan sannolikt bero på att det är svårt att utan djupare kunskaper få fram

informationen ur LISa. Det illustrerar även svårigheten att styra användning av molntjänster som enskilda medarbetare själva kan välja att använda.

Med beaktande av att Riktlinjen för informationssäkerhet anger att dokumentation ska finnas, kan det ses som ett styrningsproblem att inte alla tjänster är upptagna. När inventeringen och dokumentationen av resurser inte är komplett försvåras möjligheterna att fatta korrekta beslut gällande informationssäkerhet, samtidigt som det inte går att lämna fullständiga och korrekta uppgifter till de registrerade om behandlingen av deras personuppgifter.

En stor del av tjänsterna behandlar inga andra personuppgifter än inloggningsuppgifter till tjänsten för regionens personal. Behandling av personuppgifter är dock bara en av de regleringar som kan ställa krav på behandlingen av data. I och med införande av NIS2 kommer fler verksamheter att omfattas av förstärkta krav avseende säkerhet och riskhantering, vilket kan påverka möjligheten att behandla uppgifter i molntjänster, särskilt sådana som finns i tredje land.

Då det genomförts undersökningar av molntjänster vid två tillfällen 2022 och 2023 har jag följt upp hur de rekommendationer som funnits i de rapporterna har implementerats genom att göra stickprov I LISa. Sedan den föregående inventeringen har det skett ändringar i rättspraxis kring t.ex. säkerhetsåtgärder som pseudonymisering vilket riskerar att komplicera användning av molntjänster ytterligare. Även ett större införande av AI hos leverantörerna riskerar att skapa nya svårigheter om det inte kan garanteras att uppgifterna behandlas enbart för de syften och med de medel som regionen angivit och kan övervaka.

Problembild för molntjänster

De förekommer mer frekvent att tjänster som varit lokalt installerade antingen får nya licenstyper med abonnemang, eller har funktioner som innebär behandling i en molntjänst, Adobe är ett exempel på sådan tjänst där tilläggsfunktioner (t.ex. sammanläggning och redigering av filer) kan ske i en ansluten molntjänst utan att det är helt tydligt för användaren. När det sker uppdateringar eller uppgraderingar finns det därför anledning att se över om tjänsterna har förändrats så att behandling helt eller till del sker i molnet. Om så är fallet är det viktigt att genomföra en revision av om tjänsten uppfyller kraven och kontrollera att tjänsten kan konfigureras så att det inte uppstår problem med regelefterlevnaden.

Det har tidigare framhållits att ett område som generellt är svårt och inte får den uppmärksamhet det förtjänar, 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.)* På samma sätt bör även den personuppgiftsansvarige kontrollera att processerna och tjänsterna lever upp till de krav på säkerhet som de behandlade uppgifterna kräver.

Behandlingen av personuppgifter som utförs av en molntjänstleverantör blir typiskt sett svårare att genomföra/följa upp om kontroll och uppföljning inte planeras och införs i leveransavtalen. För att inte sådant ska utvecklas till att bli övermäktigt kan riskanalyser göras för att identifiera system och behandlingar där spårbarhet är viktig. Att förlita sig helt på leverantörernas egenkontroller kommer sannolikt inte att accepteras när behandling omfattar särskilt skyddsvärda uppgifter eller uppgifter om stora grupper registrerade.

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.

När det finns ett beroende av underleverantörer för leverans av molntjänster är det på samma sätt angeläget att även den leverantören kan följas upp och att det är dokumenterat.

Särskilda frågor om molntjänster och kravet på lämplig säkerhet

I och med att molntjänster fått en stor betydelse i många organisationer har hotaktörerna koncentrerat sig på att använda dem som en väg in för attacker. M365 har t.ex. blivit ett populärt mål för molnmedvetna hotaktörer: SharePoint och Outlook användes i 22 % respektive 17 % av relevanta intrång under första halvåret 20241, vilket understryker behovet av att inte enbart förlita sig på leverantörens säkerhetsåtgärder.

Inom cybersäkerhet anges identitets- och behörighetshantering var det som är mest utmanande och kritiska att kontrollera och skydda. Då det i tidigare undersökningar visat sig att det inte föreligger en aktiv kontroll av att medarbetare enbart har rätt behörigheter, finns en risk att medarbetare har för många och för stora behörigheter vilket kan utvecklas till ett kritiskt säkerhetsproblem.

När angripare har fått tillgång till ett IT-konto, testar de ofta åtkomsten till alla tillgängliga SSO-integrerade applikationer, särskilt de som används för chatt och videokonferenser, hantering av autentiseringsuppgifter, hantering av kundrelationer, dokumenthantering och lagring, produktivitet, ärendehantering/tickets och säkerhet. Det är därför viktigt att samtliga molntjänster övervakas för att upptäcka attacker.

Många organisationer granskar inte heller det data som anställda laddar upp till molnbaserade lagringsplatser (t.ex. SharePoint) eller överför internt via e-post, vilket gör dessa resurser till värdefulla mål för hotaktörer som försöker röra sig inom offermiljöer.

För att motverka hoten behövs kontinuerlig insyn i konfigurationer för att säkerställa att appar förblir säkra och för att stödja efterlevnad av relevanta säkerhetskrav. Nackdelen är att det förmodligen blir svårt att kombinera säkerhet med arbetsbesparande funktioner. Det behövs också en möjligheter att bättre förstå och följa de tusentals av användare som får åtkomst till

[1] Crowdstrike 2025 Global Threat report

applikationerna och de tredjepartsapplikationer som kan vara anslutna för att förbättra funktionaliteten eller arbetsflödet

Den rättsliga situationen

De rättsliga möjligheterna att använda molntjänster har blivit mer utmanade, speciellt om de kontrolleras från USA. Då det beräknas att 2/3 av de molntjänster som används inom EU kontrolleras från 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 i sig oklart i och med att flera av de principiella invändningarna rörande möjligheten för USA's myndigheter att ta del av uppgifter nu återaktualiserats. De registrerades rättigheter som nu ansetts vara lösta genom USA's utfärdande av Executive Order 14086 avseende kontrollmekanismer i syfte att stärka skyddet för den personliga integriteten står fortfarande mot övervägande om nationell säkerhet. USA's regering har dock ändrat policy i vissa avseenden och kontrollorganet PCLOB, som skulle garantera skyddet för de registrerade är inte längre är beslutsmässigt. Det kan därför ifrågasättas om förutsättningarna för adekvansbeslutet fortfarande föreligger.

Om EU-kommissionen själv eller en domstolsprövning från EU-domstolen undanröjer adekvansbeslutet kommer det inte att vara möjligt att använda lösningar från USA-baserade leverantörer, t.ex. M365 eftersom lösningen då bedöms sakna lämplig säkerhet.

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 sedan tidigare tagit fram rekommendationer
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Rekommendationen konstaterar i princip 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. Lagen om Offentlighet och Sekretess (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 utan skyddsåtgärder. De skyddsåtgärder som står till buds är i praktiken kryptering eller pseudonymisering, men även de metoderna förutsätter att leverantörerna kan visa att det finns motsvarande straffsanktionerat sekretesskydd som i Sverige om de behandlar uppgifter som kan härledas till en fysisk person. Kryptering är den metod som är säkrast men i och med att i princip ingen extern behandling kan ske utan att uppgifterna dekrypteras hos utföraren måste sekretessfrågan vara hanterad för att det ska vara genomförbart.

På sikt måste även kryptering som metod ifrågasättas om uppgifterna kan förväntas ha ett högt skyddsvärde över tid. Orsaken är att kvantkryptodatorer som på 5 till 10 år sikt med ny teknik kan dekryptera uppgifter på ett sådant sätt att de inte längre kan anses vara säkra. Konsekvenser är att uppgifter som behöver ett långtgående sekretesskydd inte bör vara exponerade mot internet eftersom de på några års sikt kommer att vara dekrypterbara även om de samlas in nu. För att förbättra skyddet bör det därför övervägas att införa PQC algoritmer för den kryptering känsliga uppgifter som kommer att hanteras i molntjänster. Självklart måste det vägas mot nyttan och behovet av att använda internetbaserad kommunikation och molnbaserade tjänstelösningar.

Det är viktigt att sekretessfrågan kan hanteras utan att exponera de ansvariga för personligt straffansvar i och med att alla externa behandlingar innebär ett utlämnande.

När det gäller användande av pseudonymisering som skyddsåtgärd har dock värdet av en sådant åtgärd blivit mer osäkert efter IMY’s beslut rörande SKR’s väntetidsdatabaser. För att metoden ska ge lämpligt skydd måste det säkerställas att hanteringen av de uppgifter som krävs för att identifiera en individ hanteras så att uppgiften inte kan åtkommas eller riskera att lämnas ut.

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 (t.ex. svårigheter att i praktiken förvalta och övervaka), vilket understryker vikten av att genomföra och dokumentera ett sådant beslut.

Microsoft M365

I och med beslutet att införa Microsoft M365 Office 365 (M365) i alla regionens nämnder och förvaltningar kommer regionens verksamhet att bli beroende av en Molntjänst, framförallt för kommunikation med mejl och virtuella möten. Beslutet har föregåtts av analyser med följd att det finns beslut om vilka typer av uppgifter som får behandlas i tjänsten, där sådana som klassas som särskilt känsliga inte får behandlas. Givet att det interna administrativa säkerhetsåtgärder (i form av informationsklassning, behörighetskontroller och loggning), kan det vara möjligt att uppnå en lämplig säkerhet för de registrerade. Det återstår dock några frågor kring möjligheterna att t.ex. leva upp till kraven för loggning givet de licenser regionen planerar att använda.

Ett potentiellt problem är dock att EU's adekvansbeslut som öppnat upp för användning i kommunal verksamhet, nu börjat ifrågasättas. Orsaken är som omnämnt ovan att USA's regering ändrat policy i vissa avseenden och kontrollorganet PCLOB, som skulle garantera skyddet för de registrerade inte längre är beslutsmässigt. Det är dock inte något som enbart påverkar regionens framtida användning av M365 utan sannolikt 2/3 av molntjänsterna för samtliga EU-länder.

I och med att det finns en osäkerhet kring de rättsliga förutsättningarna bör det vid införandet även tas fram en livscykelanalys, plan och test av hur lagrat data i M365 kan migreras tillbaka till RG eller annan plattform.

Uppföljning av rekommendationer från tidigare granskningar

2021

- Uppdatera LISa med samtliga system som innehåller personuppgifter, för system som enbart innehåller kontaktuppgifter för kommunens anställda kan det sannolikt klassas schabloniserat. Genomför riskanalyser för samtliga molntjänster som innehåller personuppgifter för brukare och kommunmedborgare.

    - I stort sett genomfört, även om det finns system som inte är dokumenterade

- Ta fram riktlinjer och instruktioner för hur uppföljning av molntjänster ska ske, samt lägg in en central regelbunden övervakning av att så sker.
    - Det saknas fortfarande centrala riktlinjer som specifikt adresserar de särskilda förutsättningar som molntjänster har.

2023

- 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.
    - Adobe och Icloud är inte införda och dokumenterade
- 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

Dokumentationen av molntjänster har till 2024 förbättrats väsentligt, även om alla molntjänster som används av regionens personal sannolikt inte är kända av IT, än mindre dokumenterade. För de system som behandlar kvalificerade personuppgifter finns det dock god dokumentation. Ett område där det av dokumentationen i LISa inte går att utläsa statusen på är rutiner för uppföljning av molntjänster, t.ex. huruvida loggar samlas in och följs upp.

Visma leverar ett flertal tjänster däribland fakturering som anges vara föremål för pågående klassificering. Då systemet är i drift måste en klassning göras, särskilt då det är känt att det föreligger ett problem med att det hanteras känsliga uppgifter med omvänt skaderekvisit i fakturaunderlagen.

Inventering 2024

De frågor som ställdes i årets inventering.

1. Vilka molntjänster som används (länk till tjänsten), om den inte finns med på den bifogade listan lägg till det längst ner på listan och lägg in en länk till tjänsten. Ange på samma sätt om ni använder en tjänst som redan finns med på listan genom att markera med JA eller skriva en kort kommentar

2. Om ni slutat använda en molntjänst som ni tidigare angett, markera den med rött

3.Om tjänsten är inlagd i LISa

4.Om det finns ett PUB avtal

MBN

MBN använder 21 molntjänster molntjänster som huvudsakligen inte behandlar känsliga personuppgifter. System kan ändå anses vara känsliga eftersom de behandlar uppgifter om ett stort antal registrerade.

PUB-avtal

Av det totalt identifierade 239 molntjänsterna återfinns 214 i LISa, varav 174 har tillräckliga uppgifter för att följas upp och där 161 har uppgifter om tecknade PUB-avtal. Det saknas således dokumentation om PUB-avtal har tecknats för över 78 molntjänster vilket ofta sammanfaller med att de inte är dokumenterade i LISa. I ett fall har DSO avrått från att teckna PUB-avtal då leverantören inte uppfyller RG's krav och skulle vara vilseledande. Då det finns ett antal PUB-avtal som tecknades i samband med att GDPR infördes kan det även finnas anledning att se över om de instruktioner som finns i PUB-avtalen återspeglar de verkliga förhållandena särskilt om det skett någon form av förändringar i behandlingen eller tjänsten.

Det finns inget krav på enskilda PUB-avtal för alla personuppgiftsansvariga nämnder, utan det som följer av Artikel 28.3 GDPR är att "Behandlingen av personuppgifter av ett personuppgiftsbiträde ska regleras i ett avtal..." , vilket möjliggör gemensamma avtal, under förutsättning att de uppfyller kraven på:

Tydlighet: Det ska framgå vilka organisationer som omfattas.

Behörighet: Alla ansvariga måste godkänna avtalet (t.ex. genom signatur, fullmakt eller konstituerande beslut).

Instruktionsrätt: Biträdet måste veta vem som får ge instruktioner – det kan utpekas i avtalet.

Underbiträden: Alla ansvariga måste ha godkänt användningen av ev. underbiträden.

Sanktioner och ansvar: Parterna bör tydliggöra ansvarsfördelning sinsemellan (även om biträdet främst är ansvarigt gentemot varje ansvarig separat).

Det är huvudsakligen RSF som tecknat PUB-avtal med leverantörerna för gemensamma tjänster, ett stickprov att befintliga avtal visar att de inte lever upp till alla de uppräknade kraven. Det som brister

är framförallt tydlighet avseende omfattning och ansvarsfördelning, främst avseende styrning av biträdet.

För molntjänster och andra outsourcade tjänster där det finns flera personuppgiftsansvariga användare inom Regionen finns ett värde i att se över hur styrning och uppföljning ska utformas för att säkerställa lämplig administrativ och teknisk säkerhet givet att kravbilden kan se olika ut för de olika nämnderna.

Slutsats

De brister som kan observeras behöver åtgärdas men utgör med något undantag inte ett hot mot de registrerades personliga integritet. De flesta nämnder använder dock idag molntjänster för HR-relaterade behandlingar, som rekrytering, vilket kan röra särskilt skyddsvärda personuppgifter. Den tillsyn som IMY genomförde mot SJ https://www.imy.se/contentassets/92d0888c4ea04c98a5b868d0f20ab7df/beslut-om-tillsynimy-2022-9442-10-0.pdf visade tydligt att kraven är detsamma även om samtliga registrerade är anställda. Då ingen särskild granskning har skett av behandlingarna för HR-ändamål uppmanas förvaltningen att själv se över om de behandlingarna kan utgöra ett problem.

På samma sätt kommer det breda införandet av MS 365 innebära att risken för felaktig behandling av personuppgifter ökar på grund av misstag. Även inom HSN finns sedan flera år en problematik med molntjänster från leverantörer som inte följer andemeningen i regleringen, men som erbjuder patienter en ökad medicinsk säkerhet. I stor utsträckning är lösningen att ansvariga för behandlingarna behöver vara aktiva med att dels ge instruktioner för hur system får användas, men även att följa upp användningen och resultatet, medvetna om att användarna kommer att lockas att använda det som är mest användarvänligt trots att det innebär risker för konfidentialitet och integritet.

Rekommendationer

För att efterleva GDPR måste alla behandlingar dokumenteras med PUB- eller annat instrument som reglerar ansvaret för behandlingen. De måste även vara dokumenterade i LISa eftersom det annars inte går att lämna korrekt information till de registrerade om behandlingarna.

Tjänsten Adobe behöver hanteras då de är lösningar som ofta innehåller personuppgifter, vilket är ett onödigt risktagande.

I och med att samtliga nämnder i någon mån kommer att använda molntjänsten M365 behöver nämnderna och den gemensamma förvaltningen göra en ansvarsfördelning och plan för hur tjänsten ska utformas, levereras, förvaltas och följas upp för att nämnderna ska kunna leva upp till sin ansvarsskyldighet. På samma sätt som det finns ett behov av att se över tydligheten i ansvar och

styrning i befintliga PUB-avtal behöver det finnas en tydlighet vad gäller ansvarsfördelning mellan nämnderna och den centrala förvaltningen, t.ex. när rättelser ska genomföras.

Det är även lämpligt att gemensamt ta fram gemensamma metoder för styrning och uppföljning med utgångspunkt i klassningen av molntjänsterna och etablera samarbeten för att förenkla och förbättra det praktiska genomförandet.

1. Genomför de förändringar som är nödvändiga för att fakturahantering inte ska behandla särskilt skyddsvärda personuppgifter.
2. Säkerställ att identifierbara personers personuppgifter inte behandlas i Adobes molnlagring.
3. Säkerställ att samtliga molntjänster som behandlar personuppgifter är dokumenterade i LISa och har ett uppdaterat PUB-avtal med instruktion som beskriver den faktiska behandlingen som utförs.
4. Säkerställ att ansvarsfördelningen mellan nämnderna och regionförvaltningen avseende förvaltning och användande av molntjänster som används av mer än en nämnd är tydligt reglerat och dokumenterat. När användningen av tjänsterna skiljer sig åt kan det behöva upprättas separata PUB-avtal för nämnderna om instruktionerna (behandlade uppgifter, gallringstider etc.) inte är desamma.
5. Gå igenom och uppdatera instruktioner för användning av molntjänster, särskilt avseende personuppgifter
6. Utse en eller flera ansvariga för uppföljning av molntjänsterna för att säkerställa att de har lämplig säkerhet och följer de instruktioner som ställts
7. Genomför uppföljning av hur molntjänster är konfigurerade avseende säkerhet och vilka uppgifter som behandlas i tjänsterna.
8. Ta fram planer för och testa att det är möjligt att migrera från molntjänster som inte längre är förenliga med de rättsliga kraven eller uppfyller kraven på lämplig säkerhet.