RAPPORT

2024 år granskningsrapport av behandling av personuppgifter på gemensamt elektroniskt lagringsmedia G: enligt Europeiska Dataskyddsförordningen (GDPR)

Fastställd av Regionstyrelsen
Framtagen av Regionens dataskyddsombud
Datum 20241218
Gäller
Ärendenr RS 2024/2232
Version 1.1

Regionstyrelsen
Region Gotland

Innehåll

Sammanfattning 2

Bakgrund 3

Gemensamma egenskaper för G: 4

Genomförande av undersökning 4

Observationer 5
Regionförvaltningen (HR) 5
Hälso- och sjukvårdsnämnden 5
Miljö- och byggnämnden 5
Socialnämnden 6
Tekniknämnden 6
Patientnämnden 6
Valnämnden 6
Överförmyndarnämnden 6
Regionförvaltningen/HR 6
DSO's bedömning 6
Förslag på åtgärder 7

SAMMANFATTNING

Region Gotlands behandling av personuppgifter i på gemensamt lagringsmedia G: uppfyller inte GDPR'S samtliga krav på teknisk och administrativ säkerhet. Det föreligger dock inte någon tydligt identifierbar risk för de registrerades personliga integritet. Bristerna består i bristande dokumentation och klassning av de uppgifter som behandlas, bristande åtkomstbegränsningar och behörighetsstyrning samt avsaknad av automatiskt stöd för utövande av de registrerades rättigheter. De registrerade får heller ingen information om att behandling av deras personuppgifter sker i systemet i enlighet med kraven i artikel 15. Bristerna måste åtgärdas främst genom att etablera dokumentation av de behandlingar av personuppgifter som förekommer och vidta kompletterande skyddsåtgärder för de uppgifter som behöver ett förstärkt skydd.

Då brister huvudsakligen kan kopplas till utformningen av den gemensamma tekniska lösningen kan med fördel bestå i en gemensam lösning även om det är möjligt att åtgärda bristerna med lokala lösningar för de respektive förvaltningarna. Problemet med efterföljnaden av GDPR är känd och det finns information på Insidan med generella anvisningar för hur det ska hanteras. Det förekommer dock en relativt stor och mindre

strukturerad behandling av personuppgifter på G:, vilket troligen kan förklaras av brist på bättre alternativ. Kommunal- och regionsverksamhet är i sig komplex och förutsätter en omfattande dokumentation som på grund av lagstiftning kan förändras med kort varsel. På samma sätt finns det ett behov av digitala verktyg för att bereda ärenden och hantera anteckningar och protokoll från möten som passar in i processerna för ärendehandläggning.

Det finns generellt ett stort behov av en lösning för lagring av dokument som kan delas med andra och som av olika skäl inte ”passar in” i verksamhetssystemen. Om en övergång sker till Office 365 kan det erbjuda en lösning avseende åtkomstkontroll och behörighetsstyrning, men troligen inte avseende de registrerades rättigheter.

Den enskilt viktigaste frågan är avseende gemensamma diskar är dock att personuppgiftsansvariga har kontroll över vilken information som behandlas och kan utöva effektiv styrning utifrån beslutade regelverk. Förvaltningarna har på en övergripande nivå god ordning på vilka uppgifter som ska behandlas men saknar effektiva möjligheter att följa upp hur G: används. I och med att det kan misstänkas förekomma mycket material som inte är nödvändigt att behandla bör detta föras över på en backup som inte är online för att minska riskerna. Ett sätt att göra det är att föra över sådana uppgifter till ett lagringsmedia som endast kan åtkommas genom att tillgång endast ges för avgränsat syfte och tid. Förslagsvis bör alla filer som införts före GDPR’s införande förutom mallar och annat material som inte innehåller personuppgifter lagras på sådant sätt. Det bör då även dokumenteras, vem som är ansvarig för dem och behörig att bevilja tillgång till dem.

Även för övriga uppgifter som behandlas på G: finns ett behov av att dokumentera strukturen över vilka handlingstyper som behandlas, syftet med behandling, vem som ansvarar för den, att de skyddas på lämpligt sätt, och att åtkomst loggas. I dagsläget saknas närmare information om behandlingen och det saknas effektiva rutiner och verktyg att följa upp behandlingarna. Det finns centralt beslutade riktlinjer för användningen, men det finns ingen dokumenterad uppföljning av behandlingen, vilket behövs för att kunna visa att säkerheten är lämplig.

Bakgrund

Dataskyddsombudet har som en del av uppdraget genomfört en granskningsaktivitet där regionens behandling av personuppgifter på ”gemensamma” lagringsytor, G-disk undersökts. Användningen av G-disk har begränsad dokumentation och ingår inte i de behandlingar som redovisas i LISa varför det varit angeläget att genomföra en begränsad genomgång. Det har i tidigare sammanhang framkommit uppgifter om att det funnits en tveksamhet kring om behandlingen uppfyller kraven som lagstiftningen föreskriver. Användningen varierar mellan de olika nämnderna, både vad avser vilken typ av information som behandlas och huruvida det finns rutiner för användningen förutom de centrala riktlinjerna.

Gemensamma egenskaper för G:

Regionens IT-avdelning är ansvarig för, förvaltar och driver IT-tjänsten. Objektsägaren är RSF IT, informationsägare i LISa är respektive nämnd/förvaltning. Tjänsten har dock en logisk uppdelning med dels en global grupp dels organisationsstyrda grupper. Det finns en instruktion på Insidan https://intra.gotland.se/sidor/stod-och-interna-tjanster/informations--och-arendehanteringsstod/gdpr-region-gotland/gemensamma-verksamhetssystem/lagringsytorna-g-med-flera.html?query=g

som anger hur information inklusive personuppgifter på G: ska hanteras. BUN, GVN och SON uppger sig ha kompletterande instruktioner t.ex. att särskilt skyddsvärda personuppgifter ska vara krypterade om de behandlas på G: Genom lösningens utformning kan användarna välja vem de vill dela dokument med utan att detta har någon centraliserad kontroll. Det finns sökfunktioner som ger användaren möjlighet att söka obegränsat i alla mappar som användaren har behörighet till. Användare med administratorsrättigheter har således åtkomst till alla uppgifter som administratörsbehörigheten avser. Loggning avseende åtkomst finns, men följs inte upp systematiserat. Då det inte finns förteckning över uppgifter eller utdelade behörigheter är det troligen inte heller meningsfullt att följa upp loggarna. På samma sätt går det inte att på ett automatiserat sätt följa upp och redovisa uppgifter enligt art 15 i GDPR.

Genomförande av undersökning

För att kunna bedöma om användningen av G-disk uppfyller kraven på lämplig administrativ och teknisk säkerhet behöver det finnas

1 kunskap om vilka personuppgifter som behandlas där

2 en fungerande styrning av att inte andra uppgifter behandlas än vad som godkänts av den personuppgiftsansvarige

3 möjlighet att uppfylla skyldigheterna mot de registrerade enligt GDPR art 12-21

4 möjligheter att begränsa och följa upp åtkomst till de personuppgifter som behandlas där

För att utvärdera lämpligheten i hur G-disk används har följande frågor ställts:

Förekommer skyddade personuppgifter?

Förekommer uppgifter om hälsa-sjukvård, socialtjänst eller andra uppgifter med omvänt skaderekvisit?

Förekommer uppgifter om brott?

Förekommer andra personuppgifter som är sekretessbelagda?

Finns instruktion för användning?

Finns möjlighet till sökning och utlämnande av uppgifter?

Finns åtkomstbegränsning?

Vem ansvarar för att bevilja åtkomst?

Finns möjlighet att följa upp åtkomst?

Finns möjlighet att återställa uppgifterna vid förlust?

Med vilken säkerhet behandlas uppgifterna?

För att kontrollera om det är möjligt att söka efter känsliga personuppgifter har även sökningar i G: gjorts, genom att söka på begrepp som t.ex. personnummer, orosanmälan.

OBSERVATIONER

Regionförvaltningen (HR)

Personuppgifter förekommer, även skyddade uppgifter och uppgifter med sekretess förekommer. Riktlinje för användning saknas.

Hälso- och sjukvårdsnämnden

Förekommer omfattande användning men mängden dokument minskar. Kan förekomma sekretesskyddade personuppgifter. Det finns ingen instruktion för användning.

Miljö- och byggnämnden

Nämnden behandlar inga särskilt skyddsvärda eller sekretessbelagda personuppgifter på G:. Det instruktion som används är den regionsövergripande. Ansvar för att bevilja behörighet avses ändras till enhetschefer.

Socialnämnden

Personuppgifter förekommer, dock inte skyddade personuppgifter uppgifter, andra uppgifter med sekretess kan förekomma i arbetsmaterial och protokoll. Riktlinje för användning finns, och inventering av personuppgifter på G: har genomförts.

Tekniknämnden

G-disk är projektavdelningens enda stödsystem. Personnummer kommer inte upp vid sökning och det bör inte förekomma uppgifter med sekretess.

Barn- och utbildningsnämnden samt gymnasie- och vuxenutbildningsnämnden

Använder inte längre G: och har flyttat uppgifterna till MS Teams. Personuppgifter är försedda med alias för att skydda integriteten, men det kan förekomma uppgifter om diagnoser och orosanmälningar. Vid sökning på orosanmälningar fanns trots ett stort antal träffar ingen känslig information.

Patientnämnden

Använder inte G:

Valnämnden

Använder inte G:

Överförmyndarnämnden

Använder G: för behandling av protokoll, och ska inte förvara personuppgifter där.

Regionförvaltningen/HR

Omfattande användning av G: för hantering av personuppgifter där behandling av skyddade personuppgifter kan förekomma, liksom andra uppgifter med sekretess så som brott, hälso-sjukvård. Det finns ingen instruktion för användning. Ingen person på HR har sökmöjligheter.

DSO'S BEDÖMNING

Nämnderna/förvaltningarna är väl medvetna om att G: inte följer GDPR's regelverk, men har i dagsläget svårt att ersätta eller åtgärda systemets brister. Den stora mängden uppgifter som bedöms finnas där speglar ett behov av lagrings och samarbetsytor som det inte finns stöd för i andra system, vilket gör att verksamheterna har ett behov som måste tillfredsställas för att det inte ska uppstå behandling i system som regionen inte har någon kontroll över, t.ex. molntjänster som Dropbox.

Det pågår i flera nämnder arbete med att minska mängden uppgifter som behandlas

vilket givetvis är bra. I och med att det generellt inte finns en inventering eller klassning av uppgifterna som behandlas i G: går det inte att uttala sig om behandlingen sker med lämplig administrativ och teknisk säkerhet, annat än att avsaknaden i sig inte uppfyller kraven. Det finns redan anvisningar på Insidan om hur arbetet ska genomföras,

För att ta ett steg mot att kunna inventera och klassa uppgifterna bör ytterligare åtgärder för rensning genomföras. Ett sätt kan vara att spara ner uppgifter som införts före 2018 offline för att på så sätt skapa en säkrare rutin för åtkomst och göra de lagrade uppgifterna mer hanterbara. Rent generellt bör det även gå att anta att uppgifter som det inte skett någon åtkomst till på ett par år inte behöver vara online, så länge som det är möjligt att få fram dem när behov uppstår.

På samma sätt bör nämnderna ge sina medarbetare i uppdrag att rensa alla personuppgifter som de inte behöver för sitt arbete eller som finns i andra system, de uppgifter och dokument som det är motiverat att spara ska då klassas och införas i LISa. När det är möjligt att bedöma vilka uppgifter som behandlas bör en automatiserad funktion för att kontrollera om en person är registrerad införas för att kunna fullgöra skyldigheterna i GDPRS artiklar 12-21. Det föreslagna åtgärderna kommer att behövas genomföra även om systemet byts ut mot t.ex. Office 365. För att säkerställa att ovanstående åtgärder utförs bör de tidsättas och vara krav för att flytta uppgifter till en ny lösning.

FÖRSLAG PÅ ÅTGÄRDER

1. De nämnder/förvaltningar som inte redan har instruktioner eller anvisningar för användning av G: bör ta fram sådana avseende användning och uppföljning
2. Ge medarbetarna i uppgift att gå igenom sina egna mappar och rensa ut allt som de inte absolut behöver ha tillgång till online. De uppgifter som fortsatt ska vara åtkomliga online på G: ska klassas och införas i LISa.
3. Flytta dokument och uppgifter där senaste ändring skedde 2018 samt sådana som inte haft någon åtkomst till en offline disk och inför en process för att kunna söka och beställa åtkomst till sådana uppgifter.
4. Genomför processkartläggning för att identifiera var handlingar på G: används i verksamheten och vem som ska vara behörig att ha åtkomst
5. Inför möjlighet att följa upp loggar för åtkomst till dokument på G:
6. Inför automatiserad möjlighet att se om registrerades uppgifter förekommer i handlingar för att kunna rendera underlag till art 15 utdrag.