

Uppföljning av nämndernas behandling av personuppgifter med AI enligt Europeiska Dataskyddsförordningen (GDPR)

Framtagen av Regionens dataskyddsombud

Datum 20260422

Gäller: Regionstyrelsen

Hälso och sjukvårdsnämnden

Socialnämnden

Barn och ungdomsnämnden

Gymnasie och vuxennämnden

Byggnadsnämnden

Tekniska nämnden

Patientnämnden

Överförmyndarnämnden

Valnämnden

Ärendenr

Version 0.5

Regionstyrelsen och nämnderna
Region Gotland

Tillsynsaktivitet nr 4 – 2025

Behandling av personuppgifter med AI

Kartläggning av AI-användning, risker och GDPR-efterlevnad

1. INLEDNING

Dataskyddsombudet (DSO) för Region Gotland genomför under 2025 tillsynsaktivitet nr 4, som avser kartläggning av hur personuppgifter behandlas med hjälp av artificiell intelligens (AI) och maskininlärning i regionens verksamheter.

AI och maskininlärning har blivit allmänt tillgängliga verktyg på mycket kort tid och kan erbjuda verksamhetsnytta, men medför också komplexa dataskyddsrättsliga

utmaningar. Eftersom både det tekniska landskapet och den rättsliga regleringen befinner sig i snabb förändring – inte minst med EU:s AI-förordning (AI Act, (EU) 2024/1689) som trädde i kraft 2024 – är kartläggning av nuläget ett nödvändigt första steg för att bedöma var fördjupat arbete krävs.

Tillsynsaktiviteten besvarar sex frågor som ställts till de granskade enheterna:

- Fråga 1 – I vilken process/för vilket syfte behandlas personuppgifter med AI?
- Fråga 2 – Vilka personuppgifter behandlas med AI?
- Fråga 3 – Används regionens databaser med personuppgifter för att träna, analysera eller fatta beslut med AI?
- Fråga 4 – Används externa databaser med personuppgifter för att träna, analysera eller fatta beslut med AI?
- Fråga 5 – Driftas AI-lösningen lokalt eller tillhandahålls den av en extern leverantör?
- Fråga 6 – Hur informeras de registrerade om att deras personuppgifter är föremål för automatiserad behandling?
-

Rapporten täcker förvaltningar och nämnder: Hälso- och sjukvårdsnämnden (HSN), Socialnämnden (SON) Regionstyrelseförvaltningen (RSF), Samhällsbyggnadsnämnden (MBN), Barn- och utbildningsnämnden och Gymnasie- och vuxenutbildningsnämnden (BUN/GVN), Tekniknämnden (TN), Patientnämnden (PAN), Valnämnden (VAN), Överförmyndarnämnden (ÖFN)

2. RÄTTSLIG RAM

2.1 GDPR och AI-behandling

Rättslig referens GDPR (EU) 2016/679, art. 5, 6, 13, 14, 22, 28, 35 | EU AI Act (EU) 2024/1689 | IMY:s vägledning om AI

Artikel 5 – Grundläggande principer

All behandling av personuppgifter, inklusive behandling via AI-system, måste följa GDPR:s grundläggande principer: laglighet, korrekthet och öppenhet (art. 5.1 a); ändamålsbegränsning (art. 5.1 b); uppgiftsminimering (art. 5.1 c); korrekthet (art. 5.1 d); lagringsminimering (art. 5.1 e); integritet och konfidentialitet (art. 5.1 f); samt ansvarsskyldighet (art. 5.2). AI-system som behandlar personuppgifter måste utformas och användas i enlighet med samtliga dessa principer.

Artikel 6 – Rättslig grund

Behandling av personuppgifter via AI kräver en giltig rättslig grund. För offentlig verksamhet är rättslig förpliktelse (art. 6.1 c) och myndighetsutövning/allmänt intresse (art. 6.1 e) de primära grunderna. Om AI-systemet används i processer som saknar anknytning till myndighetens lagstadgade uppgifter, eller om personuppgifter

matas in i en extern AI-tjänst utöver vad som är nödvändigt, kan det ifrågasättas om en rättslig grund föreligger.

Artikel 13 och 14 – Informationsskyldighet och transparens

Den personuppgiftsansvarige är skyldig att informera de registrerade om att deras uppgifter behandlas, ändamålet med behandlingen, och i förekommande fall om automatiserat beslutsfattande (art. 22). Om AI-system används på ett sätt som inte framgår av befintliga integritetspolicyer uppstår ett transparensunderskott. Integritetspolicyen på gotland.se bör återspegla faktisk AI-användning.

Artikel 22 – Automatiserat beslutsfattande

Beslut som enbart grundas på automatiserad behandling och som har rättsliga eller på liknande sätt betydande effekter för den registrerade är i princip förbjudna. Undantag finns, men kräver explicit stöd och rätt för den registrerade att begära mänsklig granskning. Kliniska beslutsstödssystem som ALMA (HSF), system som genererar handlingsrekommendationer eller rankningslistor, och automatiserade kommunikationsflöden kan potentiellt röra sig i gränslandet för art. 22.

Artikel 28 – Personuppgiftsbiträdesavtal (PUB-avtal)

När ett AI-system tillhandahålls av en extern leverantör och den leverantören behandlar personuppgifter för regionens räkning är leverantören ett personuppgiftsbiträde. Ett skriftligt PUB-avtal (data processing agreement, DPA) krävs obligatoriskt. Avtalet ska reglera bl.a. behandlingens syfte, varaktighet, uppgiftstyper, bitrådets skyldigheter och den personuppgiftsansvariges instruktioner. Avtal om att leverantören 'inte kommer åt data' eller 'inte tränar modeller' är inte tillräckliga i sig – de måste uppfylla artiklarna 28.3-kraven och dokumenteras formellt.

Artikel 35 – Konsekvensbedömning (DPIA)

En DPIA krävs när behandlingen sannolikt leder till hög risk för fysiska personers rättigheter och friheter. IMY anger att AI-system som behandlar personuppgifter i stor skala, känsliga uppgifter, eller som kan leda till diskriminering eller begränsning av rättigheter regelmässigt kräver DPIA. Användning av AI för analys, profilering eller beslutsstöd i offentlig verksamhet faller typiskt sett inom detta område.

Artikel 44 ff. – Tredjelandsoverföringar

Många AI-tjänster driftas av amerikanska leverantörer (t.ex. Microsoft, OpenAI). Personuppgifter som behandlas i deras system kan komma att överföras till tredjeland (USA). Sådana överföringar kräver lämpliga skyddsåtgärder, t.ex. standardavtalsklausuler (SCC). Det räcker inte att förlita sig på leverantörens löften om datasekretess – de rättsliga kraven ska dokumenteras och stödjas av formella avtal.

2.2 EU:s AI-förordning (AI Act)

EU:s AI Act ((EU) 2024/1689), som trädde i kraft den 1 augusti 2024 och börjar tillämpas successivt från 2025–2027, inför en riskbaserad reglering av AI-system. AI-

system klassificeras i fyra riskkategorier:

- Oacceptabel risk – förbjudna system (t.ex. social poängsättning av medborgare).
- Hög risk – system som kräver obligatorisk konsekvensanalys, dokumentation, registrering i EU-databas och mänsklig tillsyn. Hög risk inkluderar bl.a. AI i utbildning, social omsorg, personalhantering och kritisk infrastruktur.
- Begränsad risk – system med transparenskrav, t.ex. chatbottar som måste upplysa om att man interagerar med AI.
- Minimal risk – system utan specifika krav, t.ex. spamfilter.

AI Act kompletterar GDPR och de två regelverken tillämpas parallellt. Regioner och kommuner som inför AI-system i högriskklasser behöver genomföra en grundläggande rättighetskonsekvensanalys (FRIA) och registrera systemet i EU:s AI-databas. Kliniska beslutsstödssystem (som ALMA) och system som används vid rekrytering kan vara högrisk-AI.

2.3 Personuppgiftsbiträdesavtal och molntjänster

Microsoft 365/Copilot, ChatGPT och liknande molntjänster är att betrakta som personuppgiftsbiträden när personuppgifter behandlas i dem. Det är inte tillräckligt att tillförlita sig på leverantörens standardvillkor eller informella försäkringar om att data inte används för träning. Region Gotland måste säkerställa att formella PUB-avtal finns på plats, att de täcker de aktuella behandlingarna, och att tredjelandsoverföringar är reglerade.

Ett särskilt problem uppstår när medarbetare på eget initiativ använder konsumentversioner av AI-tjänster (t.ex. ChatGPT.com, Bing Chat utan inloggning) utan att detta är sanktionerat av organisationen. I dessa fall saknas ett PUB-avtal helt och hållet, och personuppgifter kan användas för träning av AI-modellerna.

3. GRANSKNINGSRESULTAT PER ENHET

3.1 Hälso- och sjukvårdsnämnden (HSN)

Svar inkom från Sofie Ohlsson, Samordnare integritetsskydd, Hälso- och sjukvårdsnämnden.

Fråga 1 – Process och syfte

Nämnden uppger att det i dagsläget inte förekommer någon behandling av personuppgifter med AI inom kärnverksamheten. Kommunikatörerna använder AI-tjänster för kommunikationsändamål, men uppger att inga personuppgifter behandlas i dessa sammanhang.

Svaret är kortfattat och lämnar övriga frågor obesvarade med hänvisning till att personuppgifter inte behandlas med AI. Det framgår dock av tillsynsaktivitet nr 2 att HSF använder ALMA – ett kliniskt beslutsstödssystem vid vårdcentralerna som läser patientinformation från journalen och

föreslår åtgärder. ALMA behandlar per definition personuppgifter, sannolikt inkl. hälsouppgifter. Om behandlingar av känsliga personuppgifter sker med ALMA behöver finns tydlig dokumentation på vad det innebär.

Fråga 2 – Personuppgifter

Inga personuppgifter uppges behandlas med AI. Se noteringen ovan avseende ALMA.

Frågor 3 och 4 – Databaser för träning/analys/beslut

Inga svar lämnas (övriga frågor lämnas 'utan kommentar'). Med tanke på att ALMA kan betraktas som ett AI-system som analyserar patientdata är det angeläget att klarlägga hur systemet klassificeras och om regionens patientdatabaser används för analys av beslutsstödet.

Fråga 5 – Drift

Inte besvarat utöver kommunikationstjänsternas externa leverantörer. Det bör klarläggas vilken leverantör som tillhandahåller ALMA och under vilka avtalsvillkor.

Fråga 6 – Information till registrerade

Inte besvarat. Patientinformationen i Region Gotlands integritetspolicy och patientinformationsblad bör inkludera information om att beslutsstödssystem som ALMA används vid patientkontakter, i enlighet med art. 13 och 14 GDPR.

Sammanfattande bedömning – HSF/HSN

HSF:s svar behöver kompletteras med uppgifter om behandlingar med ALMA, då det sannolikt utgör ett AI-system som behandlar patienters personuppgifter (inklusive känsliga hälsouppgifter) och vars GDPR-status inte har utretts i detta sammanhang. HSF behöver komplettera sitt svar och genomföra en rättslig bedömning av ALMA som AI-system, inklusive frågan om DPIA och eventuell AI Act-klassificering.

3.2 Regionstyrelseförvaltningen (RSF)

Svar inkom via Digitaliseringsavdelningen (RSF) i form av ett dokumenterat svar på de sex frågorna. RSF:s svar är det mest detaljerade av de inkomna svaren och redovisar tre distinkta AI-sammanhang: kommunikation, Microsoft 365/Copilot och AI-plattformen Intric.

Fråga 1 – Process och syfte

RSF identifierar tre användningsområden för AI:

- Kommunikation: AI-tjänster (ChatGPT for Teams, Adobe Firefly, Speech-to-text) används av kommunikatörer för att ta fram texter, bilder och ljud till gotland.se och intranätet. Information för kommunikatörer finns publicerad på Insidan.

- Microsoft 365/Copilot: CoPilot är tillgängligt i plattformen. Den licensierade delen av CoPilot är dock avstängd. Medarbetare kan använda den inbyggda varianten inom ramen för M365-plattformen för produktivitetssändamål. Riktlinjer finns för vilka uppgifter som får hanteras: öppen och intern information, inga personuppgifter.
- Intric: En upphandlad AI-plattform som utreds och pilot-testas. Front-end och back-end driftas i regionens serverhall, medan språkmodellerna driftas hos leverantör i svensk serverhall. Syftet är att erbjuda en kontrollerad AI-assistenttjänst för regionens verksamheter och därigenom minska okontrollerad användning av konsument-AI.

Utöver de dokumenterade användningarna noterar RSF att medarbetare troligen dagligen använder ChatGPT och andra webbaserade AI-tjänster och sökmotorer för administrativt stöd, utan att organisationen har kontroll över detta.

RSF:s eget konstaterande att medarbetare 'troligtvis' använder ChatGPT och webbaserade AI-tjänster 'dagligen' utan kontroll är en allvarlig signal. Om personuppgifter – även vardagliga uppgifter som namn och e-postadresser – matas in i konsumentversioner av ChatGPT (chatgpt.com) eller liknande tjänster saknas ett PUB-avtal helt och hållet, och uppgifterna kan komma att användas för träning av AI-modeller. Detta strider mot GDPR art. 28 och kan utgöra en personuppgiftsincident.

Fråga 2 – Personuppgifter

Inom kommunikationsändamålet kan följande personuppgifter förekomma: för- och efternamn, e-postadresser, telefonnummer, adresser, fastighetsbeteckningar, ärendenummer, partitillhörighet (nämndledamöter), bilder, filmer och ljud. Detta är hämtat från klassningen 'AI-tjänster Kommunikation' i LISa.

För Intric och Copilot uppges att personuppgifter inte ska matas in (policyregel). Huruvida dessa regler efterlevs i praktiken är dock inte verifierat.

Frågor 3 och 4 – Databaser för träning/analys/beslut

Tydliga svar per system:

- Kommunikation: Nej, regionens databaser används inte för träning, analys eller beslut.
- Copilot: Nej.
- Intric: Träning – Nej. Analys – Nej i nuläget, men kan bli aktuellt. Beslutsstöd – Nej i nuläget, men är möjligt framåt.

Att Intric på sikt kan komma att användas för analys av personuppgifter och som beslutsstöd är ett framåtblickande svar som är positivt ur transparensynpunkt. Det innebär att DPIA-processer och rättslig grund för sådana framtida användningar behöver planeras redan nu.

Fråga 5 – Drift

- ChatGPT for Teams, Adobe Firefly, Speech-to-text: Extern leverantör.

- Intric: Hybrid – front-end och back-end i regionens serverhall, språkmodeller hos leverantör i svensk serverhall.
- Copilot/M365: Microsoft (extern leverantör, molntjänst).

Det är positivt att Intric driftas med språkmodeller i svensk serverhall, vilket minskar risken för problematiska tredjelandsoverföringar. Det måste dock säkerställas att PUB-avtal finns för samtliga externa leverantörer.

Fråga 6 – Information till registrerade

Intric: 'Oklart, men görbart bara vi bestämmer en kommunikationsväg.' Copilot: 'Inte aktuellt då personuppgifter inte ska matas in.' Kommunikation: Inget svar.

Det saknas en samlad bild av hur de registrerade informeras om AI-baserad behandling. Personuppgifter behandlas åtminstone i kommunikationsändamålet med externa AI-tjänster, och de registrerade (allmänhet, nämndledamöter, tjänstemän vars uppgifter förekommer på gotland.se) bör informeras om detta i integritetspolicyn.

Sammanfattande bedömning – RSF

RSF:s svar är det mest heltäckande och visar att nämnden har en medveten approach till AI-användning med dokumenterade riktlinjer, central plattform (Intric) och utbildning. De primära riskerna är: okontrollerad användning av konsument-AI bland medarbetare; behov av att säkerställa formella PUB-avtal med samtliga externa leverantörer; planering av DPIA och rättslig grund inför Intrics utvidgade användning; och brist på information till registrerade om AI-behandlingen i kommunikations sammanhang.

3.3 Miljö- och byggnämnden (MBN) / Samhällsbyggnadsnämnden

Svar inkom den 25 november 2025 via Madeleine Johansson, kontaktperson GDPR (MBN 2025/859).

Fråga 1 – Process och syfte

Det finns ingen dokumenterad AI-användning i nämndens processer. Undantag: inbyggda AI-funktioner i M365 och en del medarbetare som använder ChatGPT för enklare frågor utan personuppgifter. Nämnden inväntar en regiongemensam AI-lösning.

Fråga 2 – Personuppgifter

Det uppges att frågor som ställs till AI-tjänster vanligtvis är enkla och inte innehåller personuppgifter. Angående M365: medarbetare har genomgått digitala utbildningar om vilka uppgifter som får behandlas och hur de ska hanteras beroende på typ.

Frågor 3 och 4 – Databaser för träning/analys/beslut

Nej i båda fallen. Inga databaser med personuppgifter används för träning, analys eller beslut med AI.

Fråga 5 – Drift

M365 tillhandahålls av extern leverantör (Microsoft) som molntjänst. Ingen AI-lösning driftas lokalt.

Fråga 6 – Information till registrerade

Nämnden har ingen automatiserad behandling av personuppgifter med AI i nuläget. Frågan bedöms inte som aktuell, men nämnden noterar att det kan bli relevant framöver.

Sammanfattande bedömning – MBN

MBN:s AI-användning med personuppgifter är i dagsläget minimal. Nämndens svar är kortfattat men adekvat givet den låga AI-mognaden. De primära riskpunkterna är: okontrollerad och icke-sanktionerad ChatGPT-användning bland enstaka medarbetare; behov av tydliga interna riktlinjer för vad som får hanteras i M365:s inbyggda AI-funktioner; och beredskap inför regiongemensam AI-lösning.

3.4 Barn- och utbildningsnämnden/Gymnasie och vuxennämnden (BUN/GVN)

Svar inkom den 23 oktober 2025 via Malin Karlsson, Nämndsekreterare/Verksamhetsutvecklare och GDPR-ansvarig.

Fråga 1 – Process och syfte

Inom BUN/GVN är det ett antal medarbetare som använder Microsoft Copilot. Inga specifika processer eller syften anges utöver detta – svaret är kortfattat.

Fråga 2 – Personuppgifter

De uppgifter som behandlas via Copilot är de som finns på OneDrive, Outlook och SharePoint – dvs. de personuppgifter som medarbetarna hanterar inom ramen för sina arbetsuppgifter. Inom utbildningsnämnden kan detta inkludera elevuppgifter, kommunikation med vårdnadshavare, lärares noteringar och liknande. Svaret är anmärkningsvärt kortfattat för en förvaltning vars kärnverksamhet involverar ett stort antal registrerade (elever, barn, vårdnadshavare, personal).

Riskbedömning: Om Copilot-användare inom BUN/GVN arbetar med dokument, e-post och filer som rör elever – t.ex. åtgärdsprogram, kommunikation om frånvaro, elevhälsans anteckningar – innebär detta att känsliga personuppgifter om barn potentiellt behandlas i Copilot-systemet. Detta måste utredas och dokumenteras.

Frågor 3 och 4 – Databaser för träning/analys/beslut

Nej. Regionens eller externa databaser med personuppgifter används inte för att träna, analysera eller fatta beslut med AI. CoPilot driftas av Microsoft, som uppger att de inte kommer åt data eller tränar sina modeller på data som förs in på Microsofts molnservrar.

Nämnden hänvisar till Microsofts egna löften som garanti. Det är viktigt att klargöra om det formella PUB-avtalet med Microsoft för M365/Copilot täcker den faktiska behandlingen av uppgifter inom BUN/GVN, och att avtalet uppfyller GDPR art. 28-kraven.

Fråga 5 – Drift

CoPilot ingår i regionens Office-paket och hyrs från leverantör (Microsoft). Molnbaserad tjänst.

Fråga 6 – Information till registrerade

Svaret är: *'Har inte det.'* Ingen information lämnas till de registrerade om att deras personuppgifter är föremål för automatiserad behandling via Copilot.

Art. 13 GDPR kräver att den personuppgiftsansvarige vid insamlingstillfället informerar om all behandling som sker. Om Copilot används på ett sätt som innebär att personuppgifter om elever, vårdnadshavare eller personal behandlas av systemet, men detta inte framgår av Region Gotlands integritetspolicy eller av informationen till de registrerade, föreligger en transparensbrist som utgör ett brott mot art. 13/14 GDPR.

Sammanfattande bedömning – BUN/GVN

BUN/GVN:s svar är det kortaste och minst utredda av de inkomna svaren. Det faktum att Copilot används och att de uppgifter som behandlas är allt som 'ligger på OneDrive, Outlook och SharePoint' – dvs. troligen inkl. elevuppgifter och känsliga uppgifter om barn – utan att detta är kartlagt, utrett eller kommunicerat till de registrerade, är en allvarlig brist. En fördjupad kartläggning är nödvändig.

3.5 Socialnämnden (SON)

Bedömning och svar på frågorna 1–4

Socialnämndens genomgång visar att det inte förekommer behandling av personuppgifter med hjälp av AI inom nämnden. Svaret berör frågorna 1–4 och konstaterar kortfattat att ingen AI-baserad behandling av personuppgifter pågår.

Svaret lämnar frågorna 5 (drift/leverantör) och 6 (information till registrerade) obesvarade, vilket är konsekvent med bedömningen att AI-behandling inte förekommer – dessa frågor är i så fall inte tillämpliga.

DSO:s noteringar och bedömning

Bedömningen att ingen AI-behandling av personuppgifter förekommer är lämpligt givet att genomgången.

Socialnämnden hanterar de mest integritetskänsliga uppgifterna i regionen: ärenden om barn och familjer, LVU-omhändertaganden, familjehem och ekonomiskt bistånd.

Undersökningen bör dock kompletteras med en explicit bekräftelse på att även inbyggda AI-funktioner i verksamhetssystem och eventuell informell konsument-AI-användning förekommer, vilket är den risk som övriga förvaltningar identifierat.

SON har inkommit med en komplettering

Utvecklingsledare vid SOF har skickat ut förfrågan till leverantörer av verksamhetssystem om förekomsten av inbyggda AI-funktioner. LifeCare har svarat att de inte har AI-komponenter kopplade till sitt system. Tieto kommer dock att lansera en transkriberings-tjänst inom en snar framtid – denna är inte aktiv i Lifecare utan kräver att SOF köper funktionen separat.

Regionstyrelsenämnden (RSF) har ett uppdrag från Individ- och familjeomsorgen (IFO) att utvärdera AI-komponenter för deras verksamhet. Systemet Intric är det AI-stöd som RSF tillhandahåller regionens verksamheter. Intric kan även transkribera flerpartmentmöten. Det görs en bedömning att IFO kan komma att se Tietos funktion för transkribering som säkrare, då data inte behöver flyttas ut från systemet. I dagsläget finns ingen känd tidsplan för implementering av transkriberingstöd för IFO – troligtvis som tidigast andra halvan av 2027. Funktionen är inte aktiverad i den version av IP som används inom SOF Region Gotlands verksamheter.

Övriga system (Netklient, Babonline, Treserva, Cuben) har idag inga AI-komponenter integrerade, och samtliga leverantörer har svarat att det inte heller finns någon tidplan för sådan utveckling.

Avseende informell konsument-AI-användning bedömer nämnden att det sannolikt förekommer att medarbetare använder konsumentbaserade AI-tjänster. Nämnden har dock en tydligt kommunicerad riktlinje som innebär att AI inte får användas för hantering av känslig information och/eller personuppgifter. Copilot har vid ett fåtal tillfällen identifierats som tillgängligt för verksamheten inom SOF trots RSF:s förvaltningsstyrning. Det finns tydlig kommunikation och etablerade rutiner för att när så inträffar upprätta en felanmälan till RSF, som därefter ansvarar för att utreda och korrigera avvikelsen.

Sammanfattande bedömning – SON

SON:s svar ger en klar och tydlig bild: ingen strukturerad AI-behandling av personuppgifter förekommer i dagsläget. Givet verksamhetens karaktär, med behandling av de mest känsliga uppgifterna i regionen, är detta viktigt bekräftelse. Det kvarstår ett behov av att upprätta beredskap för hantering av AI-frågor om och när sådana system eller funktioner införs av leverantörer.

3.7 Tekniska nämnden (TN)

Tekniknämnden behandlar inte personuppgifter med AI i någon process eller i något syfte.

3.8 Överförmyndarnämnden (ÖFN)

Ingen AI-behandling av personuppgifter förekommer hos nämnden.

3.9 Patientnämnden (PAN)

Ingen AI-behandling av personuppgifter förekommer hos nämnden.

4. SAMMANFATTANDE ANALYS

4.1 Inventering av AI-system per enhet

Enhet	AI-system/verktyg	Behandlar personuppg.	Extern leverantör	Träning på regiondata
HSF/HSN	ALMA (beslutsstöd)	Ja (patientdata)	Extern (okänd)	Oklar
HSF/HSN	AI-tjänster kommunikation	Nej (uppges)	Extern	Nej
RSF	ChatGPT for Teams	Ja (kommunikation)	OpenAI (extern)	Nej (avtalat)
RSF	Adobe Firefly	Ja (kommunikation)	Adobe (extern)	Nej (avtalat)
RSF	Speech-to-text	Ja (kommunikation)	Extern	Nej (avtalat)
RSF	Microsoft 365 / Copilot	Nej (policyregel)	Microsoft (extern)	Nej
RSF	Intric (AI-plattform)	Pågår (pilot)	Hybrid/SE-server	Nej
RSF	ChatGPT.com (okontrollerat)	Oklar (risk)	OpenAI (extern)	Oklar
MBN	Microsoft 365 (inbyggd AI)	Nej (uppges)	Microsoft (extern)	Nej
MBN	ChatGPT (enstaka medarbetare)	Nej (uppges)	OpenAI (extern)	Oklar
BUN/GVN	Microsoft Copilot	Ja (OneDrive/Outlook/SP)	Microsoft (extern)	Nej (uppges)

4.2 Genomgående iakttagelser

1. Okontrollerad konsument-AI är den mest akuta risken

Samtliga fyra enheter nämner att medarbetare använder eller kan tänkas använda konsumentversioner av ChatGPT och liknande AI-tjänster utan att organisationen har kontroll eller ingångna PUB-avtal. RSF konstaterar detta explicit ('troligtvis används ChatGPT dagligen'). Utan ett PUB-avtal kan personuppgifter i sådana tjänster användas för att träna AI-modeller, och Region Gotland saknar möjlighet att begära radering, insyn eller kontroll. Detta är ett omedelbart åtgärdsbehov.

2. ALMA är en olöst GDPR-fråga

ALMA, som används av HSF:s vårdcentraler, är ett AI-baserat kliniskt beslutsstödssystem som läser patientjournaler och föreslår åtgärder. Det behandlar

känsliga hälsouppgifter. HSF:s svar på tillsynsaktivitet 4 nämner inte ALMA alls, med motiveringen att inga personuppgifter behandlas med AI. Denna bedömning är sannolikt felaktig och behöver korrigeras. Frågor som behöver besvaras: Vad är Almas rättsliga grund? Finns ett PUB-avtal? Är ALMA klassificerat som högrisk-AI enligt AI Act? Har en DPIA genomförts?

3. Transparens mot registrerade saknas genomgående

Ingen av de fyra enheterna kan redovisa hur de registrerade informeras om AI-baserad behandling. BUN/GVN:s svar ('Har inte det') är det mest explicita, men bristen är generell. Art. 13 och 14 GDPR kräver att information om automatiserad behandling ges vid insamlingstillfället. Region Gotlands integritetspolicy på gotland.se måste uppdateras för att spegla faktisk AI-användning.

4. Microsoft 365/Copilot – PUB-avtal och informationsskyldighet

Tre av fyra enheter nämner Microsoft 365 och/eller Copilot. Region Gotland har ett regionövergripande avtal med Microsoft för M365, men det behöver verifieras att detta avtal täcker Copilot-funktioner och de aktuella behandlingarna. BUN/GVN:s svar är oroväckande – om Copilot bearbetar elevuppgifter i Outlook, SharePoint och OneDrive utan att de registrerade informerats föreligger en transparent- och möjligen juridisk brist.

5. RSF:s Intric-plattform är ett gott initiativ men kräver uppföljning

Digitaliseringsavdelningens satsning på en kontrollerad, regionintern AI-plattform (Intric) med språkmodeller driftade i svensk serverhall är ett strategiskt klokt steg som adresserar riskerna med okontrollerad konsument-AI. Viktiga villkor för att Intric ska uppfylla GDPR-kraven: DPIA ska genomföras innan plattformen används för personuppgifter; rättslig grund för de tilltänkta ändamålen ska fastläggas; PUB-avtal med leverantören av språkmodellerna ska upprättas; och informationskrav mot registrerade ska planeras.

4.3 Sammanfattande bedömningstabell

Enhet	F1 Process/syfte	F2 Personuppg.	F3 Egna DB	F4 Externa DB	F5 Drift	F6 Info till regist.	Samlad bedömning
HSF/HSN	Bevakas	Bevakas	Bevakas	Bevakas	Bevakas	Saknas	Otillräckligt svar – komplettera
RSF	OK	OK	OK	OK	OK	Bevakas	Bäst i klassen – kvarstående risker
MBN	OK	OK	OK	OK	OK	–	Låg risk – riktlinjer behövs
BUN/GVN	Bevakas	Brist	OK	OK	OK	Brist	Åtgärder krävs

Förklaring: Brist = identifierad brist som kräver åtgärd. Bevakas = behov av

förtydligande/komplettering. OK = uppfyllt. – = ej tillämpligt.

5. REKOMMENDATIONER OCH ÅTGÄRDER

5.1 Regiongemensamma åtgärder (alla enheter)

1. Upprätta och kommunicera en tydlig policy för AI-användning i tjänsten: vilka AI-tjänster är sanktionerade, vilka personuppgifter får hanteras var, och hur det kontrolleras. Policyn bör täcka distinktionen mellan tjänsteversioner (med PUB-avtal) och konsumentversioner (förbjudna för personuppgifter).
2. Uppdatera Region Gotlands integritetspolicy (gotland.se/personuppgifter) och relevanta personuppgiftsblad så att de speglar faktisk AI-användning, i enlighet med art. 13 och 14 GDPR.
3. Säkerställa att formella PUB-avtal (art. 28 GDPR) finns för samtliga externa AI-leverantörer där personuppgifter behandlas. Avtal ska täcka behandlingens syfte, varaktighet, uppgiftstyper och krav på radering. Microsofts standardavtal för M365/Copilot ska verifieras och dokumenteras.
4. Genomföra DPIA för AI-system som behandlar personuppgifter i stor skala, känsliga uppgifter eller som potentiellt kan leda till automatiserat beslutsfattande.
5. Genomföra utbildning för all personal om vad som gäller vid användning av AI i tjänsten, inklusive förbud mot att mata in personuppgifter i osanktionerade konsument-AI-tjänster.
6. Utse Intric eller motsvarande sanktionerad plattform som den primära kanalen för AI-assistans och kommunicera detta aktivt till medarbetare som alternativ till ChatGPT.com och liknande.

5.2 Hälso- och sjukvårdsnämnden (HSN) – Prioriterade åtgärder

7. Komplettera svaret på tillsynsaktivitet 4 med en redogörelse för ALMA-systemet: rättslig grund, PUB-avtal med leverantören, DPIA-status, och hur patienter informeras om att systemet används.
8. Genomför en klassificering av ALMA enligt EU:s AI Act. Kliniska beslutsstödssystem kan vara högrisk-AI och kräver i så fall registrering i EU:s AI-databas och löpande mänsklig tillsyn.
9. Säkerställ att de AI-tjänster som används av kommunikatörer har formella PUB-avtal och att dessa avtal är inventerade och dokumenterade.

5.3 Regionstyrelseförvaltningen (RSF) – Åtgärder

10. Genomför en riskbedömning och kartläggning av den okontrollerade ChatGPT-användningen bland medarbetare. Inför tydliga riktlinjer och tekniska åtgärder (t.ex. blockering av chatgpt.com vid behandling av personuppgifter) eller säkerställ att medarbetare enbart använder tjänsteversionen via PUB-avtal.

11. Planera och genomför DPIA för Intric-plattformen innan den tas i drift för ändamål som involverar personuppgifter, och fastslå rättslig grund för de tilltänkta användningarna.
12. Fastslå kommunikationsväg för information till registrerade om behandling via Intric och implementera detta innan produktionsdrift.
13. Verifiera att samtliga externa AI-leverantörer (OpenAI/Teams, Adobe Firefly, speech-to-text-leverantör, Intric-leverantör) har formella PUB-avtal som uppfyller art. 28-kraven.

5.4 Miljö- och byggnämnden (MBN) – Åtgärder

14. Upprätta skriftliga interna riktlinjer för vad som får och inte får hanteras i M365:s inbyggda AI-funktioner och i eventuella externa AI-tjänster.
15. Informera medarbetare om att konsumentversioner av ChatGPT och liknande inte är godkända för behandling av tjänsteuppgifter eller personuppgifter.
16. Förbered er för regiongemensam AI-lösning (Intric) och identifiera tidigt vilka processer som kan komma att involvera personuppgifter.

5.5 Barn- och utbildningsnämnden/GVN (BUN/GVN) – Prioriterade åtgärder

17. Genomför en fördjupad kartläggning av vad som faktiskt behandlas via Copilot: vilka dokument, e-postmeddelanden och filer i OneDrive, Outlook och SharePoint berör elever, vårdnadshavare eller andra registrerade?
18. Bedöm om känsliga personuppgifter (elevhälsoinformation, uppgifter om funktionsnedsättning, uppgifter om utsatta elever) förekommer i de filer och e-postmeddelanden som Copilot kan komma åt. Om så är fallet krävs DPIA.
19. Säkerställ och dokumentera att regionens PUB-avtal med Microsoft täcker Copilot-behandlingen av de uppgifter som nämnden hanterar.
20. Uppdatera information till elever, vårdnadshavare och personal om AI-baserad behandling i enlighet med art. 13 och 14 GDPR.

6. FÖRESLAGEN TIDSPLAN

Åtgärd	Enhet	Tidsgräns
Komplettera HSF:s svar med redogörelse för ALMA (AI-status, PUB-avtal, DPIA)	HSF	Omedelbart
Kartläggning av okontrollerad konsument-AI-användning och åtgärder	Alla/RSF	Inom 1 månad
Upprätta/verifiera PUB-avtal med samtliga externa AI-leverantörer	RSF, HSF, BUN/GVN	Inom 2 månader
Kartlägg vad BUN/GVN-medarbetares Copilot-användning faktiskt berör för	BUN/GVN	Inom 2 månader

uppgifter		
Genomför DPIA för ALMA (HSF) och Copilot (BUN/GVN om känsliga uppgifter berörs)	HSF, BUN/GVN	Inom 3 månader
Upprätta och kommunicera regiongemensam AI-policy för tjänsteanvändning	RSF/DSO	Inom 3 månader
Uppdatera integritetspolicy (gotland.se) med information om AI-behandling	RSF + alla enheter	Inom 3 månader
AI Act-klassificering av ALMA och andra potentiella högrisk-AI-system	HSF, RSF	Inom 4 månader
Genomför DPIA för Intric innan plattformen används för personuppgifter	RSF	Innan driftsättning
Utbildning för medarbetare om AI och GDPR	Alla enheter	Inom 6 månader
Uppföljande granskning av vidtagna åtgärder	Alla enheter + DSO	Inom 9 månader

7. SLUTSATS

Tillsynsaktivitet nr 4 visar att AI-användningen i Region Gotland fortfarande är i ett tidigt och delvis okontrollerat stadium. Den mest mogna och strukturerade hanteringen finns hos Regionstyrelsenämnden, som aktivt arbetar med en regiongemensam kontrollerad AI-plattform (Intric) och har dokumenterade riktlinjer för kommunikationsändamålet. Övriga enheter har ett mer fragmenterat och reaktivt förhållningssätt.

De tre mest angelägna riskerna som identifieras är: (1) okontrollerad användning av konsument-AI-tjänster utan PUB-avtal, vilket potentiellt exponerar personuppgifter utan rättsligt skydd; (2) ALMA-systemet hos HSF, som sannolikt är ett AI-system som behandlar känsliga patientuppgifter men som inte utretts i detta sammanhang; och (3) Copilot-användningen hos BUN/GVN, där känsliga uppgifter om barn kan vara berörda utan att de registrerade informerats.

Den regiongemensamma satsningen på Intric är ett strategiskt rätt initiativ för att minska riskerna med ad hoc-AI-användning. Det är viktigt att Intric-processen inkluderar DPIA, rättslig grundbedömning och informationskrav mot registrerade redan i pilotfasen, inte som efterhandskonstruktioner.

EU:s AI Act börjar successivt tillämpas och inför nya krav på dokumentation, registrering och mänsklig tillsyn för högrisk-AI-system. Region Gotland bör tidigt identifiera vilka AI-system som kan falla under högriskklassificeringen – ALMA är en kandidat – och påbörja arbetet med att uppfylla AI Act-kraven parallellt med GDPR-arbetet.

DSO kommer att följa upp de rekommenderade åtgärderna och genomföra en

uppföljande granskning för att säkerställa att Region Gotlands AI-användning uppfyller GDPR:s krav och är förberedd för EU:s AI-förordnings krav.