

Mottagare
Tekniska nämnden

Tillsynsrapporter - Behandling av personuppgifter

Förslag till beslut

Tekniska nämnden beslutar att ta emot informationen.

Sammanfattning

Region Gotlands dataskyddsombud har upprättat fem tillsynsrapporter under 2026. Rapporterna handlar om rättsliga grunder, barns personuppgifter, processbaserad dokumentation, AI samt molntjänster. Teknik- och samhällsbyggnadsförvaltningen kommer att vidta rekommenderade åtgärder för tekniska nämnden under 2026–2027. Förvaltningen kommer även bidra till att regiongemensamma åtgärder vidtas, genom Region Gotlands GDPR-nätverk.

Ärendebeskrivning

Under 2026 har det inkommit fem tillsynsrapporter från Region Gotlands dataskyddsombud. Rapporterna berör följande ämnen:

1. Rättsliga grunder
2. Behandling av barns personuppgifter
3. Processbaserad dokumentation
4. Behandling av personuppgifter med AI
5. Behandling av personuppgifter i molntjänster

Rättsliga grunder

Den första rapporten handlar om laglighet för behandling av personuppgifter – förekommer behandlingar utan rättslig grund?

Tekniska nämnden hanterar personuppgifter för såväl anställda, konsulter och entreprenörer som medborgare (VA, avfall, färdtjänst, boendeparkering med mera). Ingen behandling med stöd av berättigat intresse förekommer. Samtycke förekommer i två fall, kameraövervakning och Infracontrol (felanmälan). Avtal är den dominerande grunden för behandlingar som rör medborgartjänster (VA, avfall, parkering etcetera) samt anställda.

Dataskyddsombudets bedömning av tekniska nämnden:

Behov av översyn av samtliga klassningar – särskilt kameraövervakning och parallella grunder. En behandling ska ha en rättslig grund.

Rekommendation för det fortsatta arbetet med rättsliga grunder inom tekniska

nämnden:

- Utred rättslig grund för kameraövervakning och dokumentera resonemang och tillämplig lagstiftning.
- Eliminera parallella rättsliga grunder och precisera ändamålen per klassning.

Regiongemensamma åtgärder som behöver vidtas:

- Säkerställ att varje behandling har en tydlig dokumenterad rättslig grund. Parallella grunder är i regel ett tecken på att ändamålet inte är tillräckligt preciserat.
- Undvik samtycke som rättslig grund i offentlig verksamhet om det finns möjlighet att grunda behandlingen på rättslig förpliktelse, myndighetsutövning/allmänt intresse eller avtal.
- Gå igenom befintliga klassningar och uppdatera rättslig grund där det är motiverat.

Behandling av barns personuppgifter

Granskningen i den andra rapporten fokuserar på om Region Gotland uppfyller de krav som dataskyddsförordningen (GDPR) ställer när den registrerade är ett barn. Barn anses vara en särskilt sårbar grupp vars personuppgifter förtjänar stärkt skydd. Barnkonventionen, som sedan 2020 är svensk lag (SFS 2018:1197), förstärker detta perspektiv: barnets bästa ska alltid beaktas vid alla åtgärder som rör barn.

Tekniska nämnden hanterar barns personuppgifter inom tre verksamhetsområden: parkeringsautomater (betalningsuppgifter för A-traktorförare), färdtjänst och sjukresor (uppgifter med stöd i färdtjänstlagen) samt biljettsystem för kollektivtrafik (frivillig registrering för barn folkbokförda på Gotland).

Dataskyddsombudets bedömning är att tekniska nämnden hanterar barns personuppgifter i begränsad, men konkret utsträckning. Väsentliga brister: felaktig rättslig grund (avtal) för behandlingar som borde grundas på rättslig förpliktelse eller allmänt intresse; saknad artikel 9.2-grund för hälsouppgifter; avsaknad av barnspecifika rutiner och DPIA (konsekvensbedömning).

Rekommendation för det fortsatta arbetet med behandling av barns personuppgifter inom tekniska nämnden:

- Utred om sjukreseuppgifter om barn innehåller hälsodata och fastställ i så fall artikel 9.2-grund samt genomför DPIA (konsekvensbedömning).
- Granska rättslig grund för kollektivtrafik-biljettsystemet: överväg allmänt intresse (artikel 6.1 e) med stöd i kollektivtrafiklagen (2010:1065).
- Inför dokumenterade rutiner för artikel 15-utdrag och vårdnadshavarkontakt specifikt för barn.

Regiongemensamma åtgärder som behöver vidtas:

- Upprätta dokumenterade rutiner för hantering av artikel 15-begäranden avseende barn, med åldersdifferentiering som beaktar barnets mognad och rätt till integritet gentemot vårdnadshavare.
- Upprätta riktlinjer för hantering av vårdnadshavares förfrågningar om tillgång till barns personuppgifter, inkl. rutiner för verifiering av vårdnadshavarskap och hantering av oeniga vårdnadshavare.
- Säkerställa att DPIA genomförs för samtliga behandlingar av barns känsliga personuppgifter i enlighet med art. 35 och IMY:s riktlinjer.
- Genomföra utbildning för berörd personal om GDPR:s särskilda krav vid behandling av barns personuppgifter och barnkonventionens princip om barnets bästa.
- Klargöra ansvarsfördelningen för hur samtycke inhämtas för praoelever, och fastslå regiongemensamt att UAF ansvarar för processen med stöd för mottagande förvaltningar.

Processbaserad dokumentation

Granskningen i den tredje rapporten visar att tekniska nämnden ser en process (färdtjänstprocessen) som uppfyller kriterierna att behandling sker i flera system och innefattar externa parter. För övriga processer och system föreligger i grunden samma beroende till W3D3 för registrering och diarieföring.

Rekommendation för det fortsatta arbetet med processbaserad dokumentation inom tekniska nämnden:

- Dokumentation över behandlingen i processer behöver upprättas.

Regiongemensam åtgärd som behöver vidtas:

- Regionstyrelseförvaltningen bör upprätta en konkret handlingsplan med tydliga milstolpar för övergång till processorienterade klassningar. Arbetet bör samordnas med NIS2-arbetet men inte vänta på dess slutförande. En lösning för att tillåta strukturerad redovisning av flödeskedjor över flera system bör utredas inom ramen för befintliga system eller via en kompletterande dokumentationsstruktur.

Behandling av personuppgifter med AI

Granskningen i den fjärde rapporten gäller kartläggning av AI-användning, risker och GDPR-efterlevnad.

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

Regiongemensamma åtgärder som behöver vidtas:

- 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).

- 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.
- 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.
- Genomföra DPIA för AI-system som behandlar personuppgifter i stor skala, känsliga uppgifter eller som potentiellt kan leda till automatiserat beslutsfattande.
- 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.
- 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.

Behandling av personuppgifter i molntjänster

Granskningen i den femte rapporten avser den årliga tillsynsaktivitet avseende Region Gotlands användning av molntjänster som dataskyddsombudet har genomfört under 2025. Tekniska nämnden har infört några nya tjänster sedan tidigare inventering, men inga specifika avvikelser eller åtgärdsbehov har angetts utöver de regiongemensamma.

Regiongemensamma åtgärder som behöver vidtas:

- Integrera NIS2-krav med det årliga molntjänstinventeringsarbetet
- Riskklassa molntjänster ur både GDPR- och NIS2-perspektiv
- Särskilt granska tjänster med känsliga uppgifter avseende informationssäkerhetsåtgärder
- Utöka fokus på leverantörers informationssäkerhetscertifieringar (till exempel ISO 27001)
- Öka fokus på personuppgiftsaspekterna i den löpande avtalsuppföljningen

Bedömning

Bedömningen är att teknik- och samhällsbyggnadsförvaltningen kommer att vidta rekommenderade åtgärder för tekniska nämnden, enligt det som framkommer i dataskyddsombudets rapporter, under 2026 och 2027. Förvaltningen kommer även att bidra till att regiongemensamma åtgärder vidtas, genom aktivt deltagande i Region Gotlands GDPR-nätverk.

Beslutsunderlag

Tjänsteskrivelse teknik- och samhällsbyggnadsförvaltningen daterad 2026-09-28
Rapport Rättsliga grunder daterad 2026-05-04

Rapport Behandling av barns personuppgifter daterad 2026-05-04
Rapport Processbaserad dokumentation daterad 2026-04-21
Rapport Behandling av personuppgifter med AI daterad 2026-04-22
Rapport Behandling av personuppgifter i molntjänster daterad 2026-05-04

Teknik- och samhällsbyggnadsförvaltningen

Lise Langseth
Teknik- och samhällsbyggnadsdirektör

Carolina Sinander
Avdelningschef Förvaltningsstöd

Skickas till

Region Gotlands dataskyddsombud