Mottagare
Miljö- och byggnämnden

Tillsynsrapporter - Behandling av personuppgifter

Förslag till beslut
Miljö- och byggnämnden 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 miljö-och byggnämnden 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?

Miljö- och byggnämnden har en tydlig och välstrukturerad redogörelse för sina rättsliga grunder. Myndighetsutövning dominerar vid handläggning av ärenden som bygglov och miljötillsyn. Ingen behandling med stöd av berättigat intresse förekommer för närvarande, men en planerad behandling (krislistor med närmast anhöriga) har diskuterats. Samtycke används vid enstaka fotograferingar och filminspelningar av personal för intern eller extern publicering. Avtal används vid fotograferingar (modellavtal), IT-system, verksamhetssystem och kundnöjdhetsmätningar.

Dataskyddsombudets bedömning av miljö- och byggnämnden: Ingen rättslig grund ifrågasätts. Väl motiverade val. Se till att modellavtal för foto uppfyller

GDPR-krav.

Rekommendation för det fortsatta arbetet med rättsliga grunder inom miljö- och byggnämnden:

- Klargör och dokumentera ansvarsfördelningen för inhämtande av samtycke för prao-elever – fastställ om det är UAF eller mottagande förvaltning som bär ansvaret.
- Säkerställ att modellavtalen för fotografering och filminspelning av personal uppfyller GDPR:s krav avseende information, frivillighet och återkallelse.
- Följ upp och dokumentera utredningen om rättslig grund för krislistor med närmast anhöriga (om detta ska genomföras). Genomför dokumenterad riskanalys där personalorganisationerna ges möjlighet att yttra sig.

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.

Miljö- och byggnämnden behandlar i normalfallet inte barns personuppgifter. Undantag finns i tre situationer:

- Äldre bilder på barn kan eventuellt förekomma i G:-katalogen (gemensam filserver). Rensning av katalogen har påbörjats. Det finns dock ett etablerat säkerhetstänk kring fotografering av barn.
- Barn kan vara fastighetsägare och förekommer då i fastighets- och avtalsrelaterade handlingar. Denna situation är sällsynt och vårdnadshavare är alltid inblandade. Rättslig grund är rättslig förpliktelse (plan- och bygglagen) och avtal.
- Praoelever tas emot via Region Gotlands centraliserade praoprocess. Personuppgifter som behandlas är namn, telefonnummer och e-postadress. Rättslig grund är samtycke.

Dataskyddsombudets bedömning är att miljö- och byggnämnden behandlar barns personuppgifter i mycket begränsad och icke-känslig utsträckning. Hanteringen bedöms i allt väsentligt vara korrekt och proportionerlig.

Rekommendation för det fortsatta arbetet med behandling av barns personuppgifter inom miljö- och byggnämnden:

- Klargör och dokumentera ansvarsfördelningen för inhämtande av samtycke för praoelever.
- Slutför rensning av G:-katalogen för att eliminera äldre bilder på barn.
- Upprätta en dokumenterad rutin (om än enkel) för verifiering av vårdnadshavares befogenhet vid begäran om registerutdrag för barns räkning.

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 miljö- och byggnämnden har de mest utförliga processbeskrivningarna. Det är dock inte helt tydligt om flödesbeskrivningarna är inlagda i ledningssystemet för informationssäkerhet eller om de förs i ett separat register, oaktat det så uppfyller det kraven på dokumentation.

Rekommendation för det fortsatta arbetet med processbaserad dokumentation inom miljö- och byggnämnden:

- Formalisera processerna och foga dem till den löpande dokumentationen, så att de är tillgängliga vid handläggning av GDPR-ärenden. Uppgifterna om rättslig grund och lagringstid per process bör kompletteras.

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.

Miljö- och byggnämndens AI-användning med personuppgifter är i dagsläget minimal. 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.

Rekommendation för det fortsatta arbetet med behandling av personuppgifter med AI inom miljö- och byggnämnden:

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

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. Miljö- och byggnämnden 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 (exv. ISO 27001)
- Öka fokus på personuppgiftsaspekterna i den löpande avtalsuppföljningen

Bedömning

Bedömningen är att teknik- och samhällsbyggnadsförvaltningen kommer att vidta rekommenderade åtgärder för miljö- och byggnämnden, 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

TSF Tjänsteskrivelse Tillsynsrapporter behandling av personuppgifter daterad 2026-09-11
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