17 juli 2026 Kommunstyrelsen i Ånge Kommun

Granskning av dataskyddsarbete 2026

Som en del av sitt övervakande arbete och med avsikt till tillsynsplanen[1] ämnar dataskyddsombudet (DSO) att genomföra ett flertal granskningar av Sundsvall, Timrå och Ånge kommuns nämnder, bolag och förbund som använder sig av DSO tillhandahållet av Sundsvalls kommun. Granskningens syfte är att kontrollera hur Personuppgiftsansvariga (PUA) arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos PUA.

Begäran om information

Granskningen 2026 består av en enkät som fokuserar på nio olika huvudområden:

- Kontinuerlig Förbättring
- Rätt till behandlingsbegränsning
- Rätt till att invända mot behandling
- Rättigheter vid automatiskt beslutsfattande
- Personuppgiftsincidenter
- Dataskyddsombudets uppföljning av fjolårets tillsyn

Efter inlämnad enkät kan ett 30-minuters möte med dataskyddssamordnare uppkomma för att komplettera enkätens svar och ställa fördjupande frågor kopplat till inlämnat materiel.

[1] Se bifogat ” Tillsynsplan dataskydd 2026–2030”

Kontinuerlig förbättring

Målet är att:

- PUA tar regelbundet del av såväl egna som DSO:s identifierade risker och brister inom berörd del av organisationen och säkerställer samtidigt att interna regler finns för att mäta, revidera och förbättra arbetssättet.

Beskrivning av krav

Enligt dataskyddsförordningen ska PUA vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandling av personuppgifter sker i enlighet med GDPR, och dessa åtgärder ska regelbundet ses över och uppdateras vid behov. Det innebär bland annat att identifierade brister och risker i dataskyddsarbetet kommuniceras från högsta förvaltningsnivå till berörd del av organisationen så att nödvändiga åtgärder kan vidtas, samt att dataskyddssamordnare följer upp arbetet inom den egna verksamheten.

PUA bör också anta interna regler och vidta åtgärder för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard, exempelvis genom att använda godkända uppförandekoder, certifieringsmekanismer eller standarder som ISO/IEC 27001:2022 för att utvärdera och förbättra dataskyddsarbetet.

Frågor:

- Hur ofta tar PUA del av identifierade risker och brister**?**
- Vilka risker eller brister har under året kommunicerats från DSO till PUA och vidare till berörd del av organisationen?
- Har dataskyddssamordnare regelbundet deltagit i ledningsgruppsmöten eller motsvarande forum för att följa upp dataskyddsarbetet?
- Hur har identifierade brister eller risker i dataskyddsarbetet åtgärdats och följts upp under året?

Rätt till behandlingsbegränsning

Målet är att:

- PUA under utredning av frågan kan begränsa behandlingen av personuppgifter om den registrerade anser att uppgifterna är felaktiga och hen har begärt rättelse av sina uppgifter.

Beskrivning av krav

Den registrerade har i vissa särskilda situationer rätt att kräva att behandlingen av personuppgifter begränsas. Om personuppgifterna fortfarande är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats eller begäran är uppenbart ogrundad eller orimlig, får PUA neka den registrerades begäran, till exempel om den registrerade vid upprepade tillfällen begär samma sak.

Fråga:

- Finns det fastställda rutiner för hur begäran om begränsning bör hanteras?

Rätt att invända mot behandling

Målet är att:

- PUA har möjlighet, kunskap och rutiner för att kunna hantera invändningar mot PUA:s behandlingar av personuppgifter.

Beskrivning av krav

Rätten att göra invändningar gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning. Syftet med rätten att invända är att stärka den enskildes integritet och egna val.

Fråga:

- Finns det fastställda rutiner för hur begäran om invändning bör hanteras?

Rättigheter vid automatiskt beslutsfattande

Målet är att:

- PUA har möjlighet, kunskap och rutiner för att hantera automatiskt beslutsfattande på rätt sätt och säkerställer samtidigt att processen för automatiserade beslut och profilering uppfyller gällande krav.

Beskrivning av krav

Den registrerade har rätt att inte bli föremål för beslut som enbart grundar sig på automatiserad behandling, till exempel automatiskt

genererade resultat i ansökningar eller bidrag. Undantag gäller om den registrerade lämnat sitt samtycke (ej för särskilda kategorier av personuppgifter), om beslutet är nödvändigt för att ingå eller fullgöra ett avtal, eller om beslutet är tillåtet enligt lag eller EU-rätt.

Vissa personuppgiftsansvariga använder algoritmer för att fatta beslut baserat på personuppgifter. Även om detta är effektivt kan det påverka den registrerade juridiskt eller på annat sätt. När beslut fattas automatiskt ska PUA informera den registrerade om att beslutet är automatiserat, ge möjlighet att få beslutet granskat av en riktig person samt möjlighet att bestrida beslutet.

Frågor:

- Finns det fastställda rutiner för hur automatiskt beslutsfattande får genomföras?
- Använder verksamheten automatiserade beslut eller profilering?
- Om automatiserade beslut används, är processen säkerställd?

Personuppgiftsincidenter

Målet är att:

- Personuppgiftsincidenter dokumenteras och följs upp systematiskt, och incidenter som ska anmälas till Integritetsskyddsmyndigheten (IMY) hanteras inom 72 timmar.

Beskrivning av krav

En personuppgiftsincident kan få allvarliga konsekvenser för registrerade personer. De kan råka ut för till exempel ekonomisk skada eller kränkning av sina fri- och rättigheter. En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan också påverka tilltron till den organisation som behandlar personuppgifter. Det kan dessutom leda till sanktionsavgifter.

Enligt GDPR ska PUA vid allvarligare incidenter anmäla incidenten till tillsynsmyndigheten IMY inom 72 timmar från tidpunkten då den blev känd. Det krävs därför att organisationen har rutiner för att upptäcka personuppgiftsincidenter samt kunskap om vad som är en personuppgiftsincident.

I vissa falla ska även den registrerade, vars personuppgifter incidenten avser, få information om incidenten så att hen kan agera

och vidta åtgärder. Organisationen behöver ha rutiner för att göra riskbedömningar samt förutsättningar för att lämna information till den registrerade.

Frågor:

- Finns tydliga rutiner för att snabbt och enkelt kunna hantera personuppgiftsincidenter?
- Har PUA haft incidenter som rapporterats till IMY?

Dataskyddsombudets uppföljning av fjolårets tillsyn

Målet är att:

- Att följa upp utfärdade rekommendationer från dataskyddsombud till den personuppgiftsansvarige.

Beskrivning av krav:

Enligt GDPR ska Dataskyddsombudet övervaka efterlevnaden av dataskyddsförordningen. Det kan till exempel innebära att dataskyddsombudet samlar in information om hur personuppgifter behandlas i organisationen och utfärdar rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Fråga:

- Beskriv vilka åtgärder som har vidtagits och vilka åtgärder som kvarstår efter 2025s tillsyn.

Era svar

Skicka era svar skriftlig till dataskyddsombud@sundsvall.se senast den 9 november 2026.

Om ni utöver svaren på våra frågor vill hänvisa till ytterligare information så ange detta och vad ni vill visa med dem och bifoga gärna informationen med svaren.

Har ni frågor kontakta:

Camilla Eriksson
Dataskyddsombud
072-146 51 19
dataskyddsombud@sundsvall.se