16 juli 2025 Valnämnden i Ånge Kommun

Granskning av dataskyddsarbete 2025

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 2025 består av en enkät som fokuserar på nio olika huvudområden:

- Utbildning/medvetenhet/följsamhet och kultur
- Rätt till rättelse
- Rätt till radering
- Register över behandlingar
- Dataskyddsorganisation
- Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal
- Personuppgiftsbiträden och underbiträdens arbete med GDPR
- Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet
- 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 2023–2027”

Utbildning/medvetenhet/följsamhet och kultur

Målet är att:

- Säkerställa rätt kompetens hos alla medarbetare utifrån deras roll.
- Utbildning i dataskydd sker regelbundet.
- Medarbetare känner till sina generella fri- och rättigheter.
- PUA:s processer för dataskydd är kända för alla medarbetare

Beskrivning av krav:

Utöver formalia med dokumenterade och beslutade styrdokument och processer är en förutsättning till regelefterlevnad att kunskapsnivån om dataskyddslagstiftningen och interna arbetssätt är tillräckligt hög. Genom att öka medvetenhet och kunskap om personuppgiftshantering så kommer riskerna som finns med hanteringen troligtvis att minska, efterlevnad av regler blir bättre, och acceptansen och förståelsen för dataskyddsfrågor i stort öka.

PUA ska därför skapa relevanta, uppdaterade utbildningar för medarbetare, beroende på roll och arbetsuppgifter samt säkerställa att de har den kompetens och kunskap som krävs för sina arbetsuppgifter.

Frågor:

- I vilken utsträckning och form får nyanställda utbildning/information om GDPR?
- Finns det dokumentation över vilken utbildning som anställda har fått om GDPR?
- När senast genomfördes utbildning?

Rätt till rättelse

Målet är att:

- Den registrerade har rätt till rättelse, Denna rättighet medför skyldighet för organisationen och det krävs att organisationen har kunskap och rutiner för att tillgodose dem.

Beskrivning av krav:

Den registrerades rättigheter regleras av GDPR och omfattar lagstadgade rättigheter som individen kan åberopa gentemot personuppgiftsansvarig (PUA). Rätten till rättelse innebär att den registrerade, under vissa förutsättningar, har rätt att få felaktiga personuppgifter korrigerade samt att få ofullständiga uppgifter kompletterade. Organisationer är skyldiga att möjliggöra detta på ett enkelt och kostnadsfritt sätt, utan onödigt dröjsmål.

Fråga:

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

Rätt till radering

Målet är att:

- Den registrerade har rätt till radering av information. Denna rättighet medför skyldighet för organisationen och det krävs att organisationen har kunskap och rutiner för att tillgodose dem.

Beskrivning av krav:

Rätten till radering, eller ”rätten att bli bortglömd” innebär att registrerade, utifrån vissa förutsättningar, har rätt att få sina personuppgifter raderade. Organisationer behöver dock inte radera personuppgifter om uppgifterna behövs för att fullfölja avtal eller avsluta ett ärende med den registrerade. Personuppgifterna får inte heller raderas om det finns lagar, förordningar, föreskrifter eller andra offentliga förlägganden som föreskriver annat. Varje registrerad ska underrättas i samband med att deras personuppgifter raderas eller anonymiseras.

Fråga:

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

Register över personuppgiftsbehandlingar

Målet är att:

- Det finns en registerförteckning som uppdateras och revideras minst årligen.

Beskrivning av krav:

PUA är skyldiga att föra ett skriftligt register över personuppgiftsbehandlingar. Bestämmelsen innehåller dels vad som ska finnas med (formkrav), dels vissa krav om kvaliteten på innehållet. Som exempel ska ändamålet med personuppgiftsbehandlingen anges och inte ändamålet med ett system. En fullständig registerförteckning är en förutsättning för ett godkänt dataskyddsarbete. Registerförteckningen medför också en god överblick och kontroll beträffande vilka personuppgiftsbehandlingar som görs inom organisationen. Det underlättar bland annat vid begäran om registerutdrag från den registrerade. Tillsynsmyndigheten kan komma att efterfråga registret som då ska kunna göras tillgängligt för dem.

Frågor:

- Har ni ett register över personuppgiftsbehandlingar?
- Hur många behandlingar har ni i registret?
- När uppdaterades registret senast?

Dataskyddsorganisationen

Målet är att:

- Ansvar och roller för det systematiska dataskyddsarbetet finns och är kända i verksamheten.

Beskrivning av krav:

Även om det inte framgår i GDPR att en dataskyddsorganisation måste finnas så finns det ett tydligt krav på att lämpliga organisatoriska säkerhetsåtgärder ska vidtas. Däremot ett systematiskt och metodiskt dataskyddsarbete görs lämpligaste i en dataskyddsorganisation. Detta hänger också ihop med PUA:s ansvarsskyldighet att visa hur de följer dataskyddsförordningen.

Fråga:

- Har ni dokumenterat, beslutande dataskyddsorganisationer, med rollbeskrivning, ansvar och avsatt tid för medverkande personer?

Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal

Målet är att:

- PUA har aktuella personuppgiftsbitädesavtal med personuppgiftsbiträden, datadelning om det föreligger ett gemensamt personuppgiftsansvar och samarbetsavtal inom kommunkoncernen.

Beskrivning av krav:

PUA och personuppgiftsbiträden ska upprätta ett så kallat personuppgiftsbiträdesavtal om biträden behandlar personuppgifter för PUA:s räkning. GDPR räknar upp vad ett sånt biträdes ska innehålla.

Vid gemensamt personuppgiftsansvar ska ett datadelningsavtal upprättas och inom kommunkoncernen ska personuppgiftsbiträdesavtal benämnas överenskommelser. Alla personuppgiftsbiträdesavtal, datadelningavtal och överenskommelser ska dokumenteras och vara sökbara.

Frågor:

- Finns det en rutin för hur avtal/överenskommelser upprättas (vem, hur, när avtalet dokumenteras)?
- Går det att hitta avtalen/överenskommelser?

Personuppgiftsbiträden och underbiträden och underbiträdens arbete med GDPR

Målet är att:

- PUA säkerställer att det finns avtal med personuppgiftsbiträden och underbiträden och de efterlever avtalen och GDPR.
- PUA regelbundet följer upp att personuppgiftsbiträden efterlever de personuppgiftsbiträdesavtal som har ingåtts.

Beskrivning av krav

Enligt GDPR ska PUA enbart anlita personuppgiftsbiträden som kan lämna tillräckliga garantier för att de genomför tekniska och organisatoriska åtgärder som lever upp till kraven i GDPR. PUA ska följa upp att deras personuppgiftsbiträden och underbiträden efterlever de personuppgiftsbiträdesavtal som har ingåtts och kunna vis att kontroller genomförts.

Frågor:

- Granskar PUA personuppgiftsbiträdens efterlevnad av sina avtal?
- Tar PUA hänsyn till eller ställer krav på ”inbyggt dataskydd” när ni väljer tjänster och produkter att använda för behandling av personuppgifter.
- Finns det genomförda konsekvensbedömningar för de flesta systemen?

Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet

Målet är att:

- Systemen som kommunen använder sig av är säkra och lagliga, det tekniskt möjligt att begränsa åtkomst, följa upp spårbarheten och skydda känslig information med kryptering eller flerfaktorsautentiseringar.
- Tekniska och organisatoriska säkerhetsåtgärder ses över kontinuerligt.

- Det finns rutiner för tilldelning och avslutande av behörighet i samband med anställning, avslutande av tjänst/byte av tjänst.
- Ett ledningssystem för informationssäkerhet är att implementerat och genomgår ständiga förbättringar.

Beskrivning av krav:

Enligt GDPR ska personuppgifter skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga. Det är PUA:s ansvar att genomföra dessa tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med GDPR.

Den personuppgiftsansvariga ska även se över åtgärder och uppdatera dem vid behov. Exempelvis bör det finnas rutiner för hur behörigheter tilldelas och avslutas och det bör ställas krav på verksamhetssystem att det finns möjlighet att styra behörigheter i dem.

Det ska även finnas en förmåga att fortlöpande säkerställa konfidentialitet, riktighet, tillgänglighet och spårbarhet i behandlingsystem och tjänsterna. Det vill säga att bland annat säkerställa redundans, upprätta brandväggar & antivirus och ha en förmåga att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.

Fråga:

- Finns det rutiner för tilldelning och avslutande behörigheter i samband med anställning, avslutande av tjänst/byte av tjänst?
- Finns det möjlighet att begränsa behörigheten i verksamhetssystemen?
- Finns rutiner för behörighetsstyrning till alla system där personuppgifter behandlas?

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.

Frågor:

- Beskriv vilka åtgärder som har vidtagits och vilka åtgärder som kvarstår efter 2024s tillsyn.

Era svar

Skicka era svar skriftlig till dataskyddsombud@sundsvall.se senast den 14 november 2025.

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