Sundsvalls kommun

Valnämnden i Ånge Kommun **5 augusti 2024**

Granskning av dataskyddsarbete 2024

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 2024 består av en enkät som fokuserar på sju olika huvudområden:

- Rättslig grund för personuppgiftshantering
- Rätt till information
- Samtycke/samtyckesprocess
- Rätt till tillgång
- Personuppgiftsincidenter
- Konsekvensbedömningar
- Personuppgiftsprocesser och tredjelandsöverföringar
- 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”

Rättslig grund för personuppgiftsbehandlingar

Målet är att:

- Rättslig grund finns dokumenterad för varje personuppgiftsbehandling.

Beskrivning av krav

Av GDPR framgår att minst en av de sex angivna, rättsliga grunderna ska finnas för varje personuppgiftsbehandling och dokumenteras i personuppgiftsbehandlingsregistret. Rättslig grund ska även anges i PUA:s integritetsmeddelanden (externt och internt).

Den rättsliga grunden ska kunna kopplas till varje behandling och varje behandling är bunden av ett, på förhand, uttryckligt ändamål/syfte. I ett och samma system kan den rättsliga grunden variera för de olika behandlingarna. Som exempel kan nämnas att inom personaladministration kan det dels förekomma behandlingar med ändamålet att redovisa underlag till Skatteverket, den rättsliga grunden är då rättslig förpliktelse, dels kan det förekomma behandlingar med ändamålet att betala ut lön, den rättsliga grunden är då sannolikt avtal (anställningsavtal).

Frågor:

- Finns det rättsliga grunder för varje behandling av personuppgifter samt om behandlingen involverar känsliga personuppgifter i registerförteckningen?
- Vilka rättsliga grunder använder verksamheten?

Rätten till information

Målet är att:

- Kunskap och rutiner finns för hantering av ”rätten till information”.

Beskrivning av krav:

PUA ska informera om att personuppgiftsbehandling sker behandlingen när uppgifterna samlas in eller vid första kontakttillfället om de samlas in från någon annan.

Informationen ska innehålla vilka ändamål personuppgifter inhämtas för, den rättsliga grunden för behandlingen, hur länge personuppgifterna kommer att lagras, vem som kommer att få ta del av personuppgifterna, den registrerades rättigheter, om personuppgifterna kommer att överföras till tredje land, hur man lämnar klagomål till tillsynsmyndigheten, att samtycke i tillämpliga fall kan återkallas samt kontaktuppgifter till PUA och eventuellt DSO.

Frågor:

- Finns informationen på alla ställen där personuppgifter samlas in? (t.ex. på blanketter eller som länk i e-tjänster)
- Är information lätt att läsa och ta till sig? Gör 3 stickprov

Samtycken/samtyckesprocess

Målet är att:

- Säkerställa att de behandlingar som omfattas av samtycke som rättslig grund följer lagens krav och att processen fungerar.

Beskrivning av krav:

Den rättsliga grunden samtycke innebär att den registrerade har sagt ja till personuppgiftsbehandlingen. Men i många fall är det inte en lämplig grund att stödja sig på. PUA bör därför alltid överväga om ni kan använda någon av de andra rättsliga grunderna.

Ett samtycke från registrerade måste vara frivilligt. Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter. Samtycket blir därför ogiltigt om någon har utsatts för påverkan. Den registrerade får inte heller drabbas av negativa konsekvenser om hen inte lämnar sitt samtycke. Samtycket får heller inte vara en obligatorisk del av avtalsvillkor.

Det ska vara lika lätt att återkalla ett samtycke som att lämna det. Det är särskilt viktigt när det gäller barn. Samtycket ska också dokumenteras av PUA.

Frågor:

- Om ni förlitar er på samtycke för behandling av personuppgifter, följer ni GDPR:s samtyckeskrav som är: specifikt, informerat, lämnat för ett specifikt ändamål samt lätt att ta tillbaka?
- Ställer PUA krav på den registrerade i samband med samtycket? Det vill säga att den registrerade direkt eller indirekt måste ge en motprestation för tjänsten eller varan, till exempel godta vissa användarvillkor eller affärsvillkor.
- Om organisationen använder sig av samtycke, beskriv rutinen för hantering av samtycken.

Rätten till tillgång

Målet är att:

- Rätten till tillgång innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas för att kunna ha kontroll över sina egna uppgifter. Informationen ska lämnas i ett så kallat registerutdrag.

Beskrivning av krav

Rätten att få en kopia på personuppgifter innebär inte att man har rätt att få ut själva handlingen där personuppgifterna förekommer. Det kan ofta vara tillräckligt att PUA ger en begriplig sammanställning av de personuppgifter som förekommer i handlingen eller i övrigt är under behandling så att den registrerade kan kontrollera uppgifternas riktighet och laglighet. Rätten till tillgång ska inte blandas ihop eller likställas med rätten att ta del av allmänna handlingar från en myndighet. PUA ska återkomma till den registrerad utan onödigt dröjsmål och senast inom en månad efter att ha fått in begäran.

Frågor:

- Finns det fastställda rutiner för hur begäran om registerutdrag bör hanteras?
- Har ni fått begäran om registerutdrag? Hur har ni hanterat denna?
- Svarar PUA i rätt tid?

Personuppgiftsincidenter

Målet är att:

- Personuppgiftsincidenter dokumenteras och följs upp på ett systematiskt sätt.
- Personuppgiftsincidenter som ska anmälas till 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?
- Finns det tillräckligt med kunskap inom organisationen för att identifiera personuppgiftsincidenter?

- Har PUA haft incidenter som rapporterats till IMY?
- Hur många personuppgiftsincidenter har skett januari-juni 2024?

Konsekvensbedömningar

Målet är att:

- Innan en ny personuppgiftsbehandling påbörjas, kunna genomföra analyser och bedöma risker, vilket skapar bättre förutsättningar för att värna om den registrerades personliga integritet.

Beskrivning av krav

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska PUA före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

PUA ska skydda enskildas rättigheter och friheter vid särskilt riskfyllda personuppgiftsbehandlingar och se till att behandlingen är laglig samt kunna visa det.

PUA ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförandet av en konsekvensbedömning avseende dataskydd.

Frågor:

- Har det genomförts någon konsekvensbedömning och i så fall hur många? (inkl. så kallad mini-konsekvensbedömningar)
- Hur har de genomförts, i vilket system, i pappersform?
- Finns tydliga rutiner för att enkelt kunna genomföra en konsekvensbedömning avseende dataskydd?

Personuppgiftsprocesser och tredjelandsöverföringar

Målet är att:

- Överföringar till länder utanför EU och EES-området eller internationella organisationer är riskfyllda och ställer stora krav på organisationen i de fall EU-kommissionen inte har bedömt att landet eller den internationella organisationen har en adekvat skyddsnivå.

Beskrivning av krav

Tredjelandsöverföringar avser när personuppgifter behandlas i tredjeland, dvs. land utanför EU/EES. Med behandling avses dels överföring, dels åtkomst till och från tredjeland. Det är inte ovanligt att molntjänstsystem såsom lagring, kommunikation eller ärendehantering medför överföring till tredjeland. Utgångspunkten är att samtliga tredjelandsöverföringar är otillåtna om inte någon av undantagsbestämmelserna i GDPR medger annat. Det spelar med andra ord ingen roll vilka tekniska och organisatoriska säkerhetsåtgärder en organisation anser sig vidtagit för att möjliggöra tredjelandsöverföring. Förbudet mot tredjelandsöverföringar gör heller ingen skillnad på om det handlar om ”vanliga” eller ”enkla” personuppgifter eller om en organisation själv bedömer att personuppgifterna inte är kränkande.

Frågor:

- Finns det kunskap över vilka länder anses vara tredjeländer?
- Finns det leverantörer eller underleverantörer i tredje land i er verksamhet?
- Hur ser processen ut för tredjelandsöverföringar, när man anlitar en ny leverantör?
- Är verksamheten medveten om tredjelandsöverföringar och vad de innebär?

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 2023s tillsyn.

Era svar

Skicka era svar skriftlig till dataskyddsombud@sundsvall.se senast den 15 november 2024.

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