Tillsynsplan dataskydd

2026-2030

Titel: Dataskyddsombud

Organisation: Kommunstyrelsen

Diarienummer: Ange diarienummer

Innehåll

Tillsynsplan dataskydd....2
Organisationer som ingår i tillsynsplanen....2
Sammanställning år 2026-2030 4
År 1 – 2026 6
År 2 – 2027 10
År 3 – 2028 18
År 4 – 2029 24
År 5 – 2030 30

Tillsynsplan dataskydd

Dataskyddsombudet (DSO) avser att genomföra granskningar av Sundsvall, Ånge och Timrås organisationers efterlevnad av dataskyddsförordningen (GDPR). Granskningarna gäller för de nämnder, bolag och förbund som använder sig av DSO tillhandahållet av Sundsvalls kommun. Granskningar kommer genomföras löpande under år 2026–2031 och planen kommer att uppdateras inför varje nytt år.

Årligen kommer DSO att lämna en rapport som sammanfattar samtliga granskningsåtgärder som vidtagits under det gångna året. Rapporten lämnas till personuppgiftsansvarig organisation. DSO kan även komma att lämna löpande redogörelser under perioden avseende GDPR-efterlevnad.

DSO rekommenderar att respektive personuppgiftsansvariga (PUA) tar tillsynsplanen i beaktande vid planeringen av GDPR-arbetet nästkommande år.

Organisationer som ingår i tillsynsplanen

Utgångspunkten är att alla organisationer inom dataskyddsamarbetet i Sundsvall, Timrå och Ånge kommun ska ingå och kommer får samma typ av granskning enligt beskrivning i detta dokument.

Personuppgiftsansvariga organisationer:

Sundsvall

Organisation	Namn
Bolag	Mitthem AB
Bolag	MittSverige Vatten och Avfall AB
Bolag	Servanet AB
Bolag	SKIFU AB
Bolag	Stadsbacken AB
Bolag	Sundsvall Timrå Airport
Bolag	Sundsvalls Elnät AB
Bolag	Sundsvalls Energi AB
Bolag	Sundsvalls Hamn AB
Bolag	Sundsvalls Oljehamn AB
Förbund	Medelpads Räddningstjänstförbund

Nämnd	Barn- och utbildningsnämnden
Nämnd	Individ- och arbetsmarknadsnämnden
Nämnd	Kommunstyrelsen
Avdelning	HR Avdelningen, Kommunstyrelsen
Nämnd	Kultur- och Fritidsnämnden
Nämnd	Lantmäterinämnden
Nämnd	Miljönämnden
Nämnd	Stadsbyggnadsnämnden
Nämnd	Valnämnden
Nämnd	Vård- och omsorgsnämnden
Nämnd	Överförmyndarnämnden

Timrå

Organisation	Namn
Bolag	Timråbo AB
Nämnd	Barn- och utbildningsnämnden
Nämnd	Kommunstyrelsen
Avdelning	HR Avdelningen, Kommunstyrelsen
Nämnd	Kultur- och tekniknämnden
Nämnd	Miljö- och byggnadsnämnden
Nämnd	Socialnämnden
Nämnd	Valnämnden

Ånge

Organisation	Namn
Bolag	Ånge Energi AB
Bolag	Ånge Fastighets och Industri AB
Nämnd	Kommunstyrelsen
Avdelning	HR Avdelningen, Kommunstyrelsen
Nämnd	Myndighetsnämnden
Nämnd	Valnämnden

Sammanställning år 2026–2030

Rubrik	-26	-27	-28	-29	-30
Struktur, rutiner och processer		X			X
Dataskyddsorganisation		X		X	
Utbildning, medvetenhet och främjande av dataskyddskultur		X		X	
Kontinuerlig förbättring	X			X	
Rättslig grund för personuppgiftshantering		X			X
Lagringsminimering och gallring		X			X
Övriga principer		X			X
Rätt till information		X			X
Samtycke och samtyckesprocess		X			X
Rätt till tillgång		X			X
Rätt till rättelse och rätt till radering			X		
Rätt till behandlingsbegränsning	X			X	
Rätt till dataportabilitet			X		
Rätt att invända mot behandling	X			X	
Rättigheter vid automatiserat beslutsfattande	X			X	
Register över personuppgiftsbehandlingar			X		
Personuppgiftsincidenter	X		X		X
Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal			X		
Personuppgiftsbiträdens och underbiträdens arbete med GDPR			X		
Konsekvensbedömningar		X		X	
Tredjelandsöverföringar			X		
Tekniska och organisatoriska säkerhetsåtgärder och proportionalitet			X		
Dataskyddsombudets uppföljning av fjolårets tillsyn	X	X	X	X	X

Genomförande och redovisning

Granskningen består huvudsakligen av en enkät, men kan även kompletteras med intervjuer, styrdokument och stickprovskontroller. Stickprov kan genomföras på e-tjänster och blanketter för att säkerställa att korrekt information till de registrerade finns tillgänglig. Vidare kan stickprov genomföras för att kontrollera att erforderliga personuppgiftsbiträdesavtal har tecknats. Stickprov kan även omfatta verksamhetssystem.

Varje granskningsområde omfattar ett mål, en beskrivning av krav samt underlag med frågeställningar.

Resultatet av granskningen dokumenteras i en skriftlig rapport med rekommendationer till PUA:s högsta förvaltningsnivå.

År 1 – 2026

Granskningen avser:

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

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.

År 2 – 2027

Granskningen avser:

- Struktur, rutiner och processer
- Dataskyddsorganisation
- Utbildning, medvetenhet och främjande av dataskyddskultur
- Rättslig grund för personuppgiftshantering
- Lagringsminimering och gallring
- Övriga principer
- Rätt till information
- Samtycke och samtyckesprocess
- Rätt till tillgång
- Konsekvensbedömningar
- Dataskyddsombudets uppföljning av fjolårets tillsyn

Struktur, rutiner och processer

Målet är att:

- Organisationen har ekonomiska och personella resurser för ett systematiskt dataskyddsarbete som är anpassat till mängden och typen av personuppgiftsbehandlingar, där dataskydd är integrerat i verksamheten, dokumenterat och bedrivs på ett systematiskt sätt.

Beskrivning av krav

Dataskyddsförordningen kräver att organisationer genomför och löpande underhåller ett strukturerat dataskyddsarbete. Det innebär bland annat att ta fram dokumentation, besluta om styrdokument, införa processer för dataskydd och säkerställa att medarbetare har

tillräcklig kunskap, exempelvis för att kunna identifiera och rapportera personuppgiftsincidenter.

Personuppgiftsansvarig (PUA) ansvarar för att skapa förutsättningar för detta arbete genom att säkerställa resurser, planering samt lämpliga tekniska och organisatoriska åtgärder. Åtgärderna ska anpassas efter behandlingens risker och regelbundet följas upp. För att uppfylla ansvarsskyldigheten enligt GDPR behöver organisationen också ha relevanta styrdokument, rutiner och processer som integrerar dataskydd i verksamhetens ordinarie arbete.

Frågor:

- Finns det en beslutad verksamhetsplan, årsplan eller handlingsplan för organisationens dataskyddsarbete?
- Är organisationens rutiner och processer för dataskydd dokumenterade?
- Hur säkerställs att dataskydd integreras i verksamhetens ordinarie arbete (t.ex. genom styrdokument, rutiner eller utbildning)?

Dataskyddsorganisation

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 systematisk och metodisk dataskyddsarbete görs lämpligast i en dataskyddsorganisation. Detta hänger också ihop med PUA:s ansvarsskyldighet att visa hur de följer dataskyddsförordningen.

Fråga:

- Har ni en dokumenterad, beslutad dataskyddsorganisation, med rollbeskrivning, ansvar och avsatt tid för medverkande personer?

Utbildning, medvetenhet och främjande av dataskyddskultur

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?

Rättslig grund för personuppgiftsbehandlingar

Målet är att:

- Rättslig grund finns dokumenterad för varje personuppgiftsbehandling.
- Intresseavvägningar är dokumenterade.

- Samtycken är dokumenterade på rätt sätt och kan återtas.

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:

- Dokumenterar och motiverar PUA på ett lämpligt sätt er rättsliga grund för behandling av personuppgifter samt om behandlingen involverar känsliga personuppgifter eller uppgifter om brott?
- Är information om ändamålet med behandlingen och den rättsliga grunden allmänt tillgänglig, lätt att hitta, komma åt och läsa?

Lagringsminimering och gallring

Målet är att:

- Personuppgifter raderas eller avidentifieras för varje personuppgift som inte längre behövs för ändamålet. Undantaget är personuppgifter som måste sparas i enlighet med annan lagstiftning. Gallring ska genomföras för att leva upp till principen om lagringsminimering.

Beskrivning av krav

PUA får spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När personuppgifterna inte längre behövs för ändamålet ska de raderas eller avidentifieras. PUA ska

därför införa rutiner för gallring av personuppgifter, till exempel att genomföra regelbundna kontroller eller radering efter viss tid.

I vissa fall måste handlingar som innehåller personuppgifter sparas även efter det att PUA slutat använda dem. Det gäller till exempel bokföring, där bokföringslagen ställer krav på hur länge vissa handlingar ska sparas. Lagra då handlingarna på ett sådant sätt att de inte längre är tillgängliga i den dagliga verksamheten, det vill säga avskilj personuppgifterna.

Det kan också vara tillåtet att lagra personuppgifter när det ursprungliga ändamålet inte längre är aktuellt, om det sker för:

- arkivändamål av allmänt intresse
- vetenskapliga eller historiska forskningsändamål
- statistiska ändamål.

Frågor:

- Fungerar gallring, avskiljning och arkivering?
- Finns beslutade gallringstider?
- Utförs gallring i system och i ostrukturerat material (Outlook, Intranät, Teams) i enlighet med interna styrdokument?

Övriga principer

Målet är att:

- Säkerställa att GDPR efterlevs inom alla principer.

Beskrivning av krav

Ändamålsbegränsning – säkerställa att personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska inte anses vara oförenlig med de ursprungliga ändamålen.

Uppgiftsminimering – säkerställa att personuppgifter är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Riktighet (korrekthet) – säkerställa att personuppgifter är riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Integritet och konfidentialitet – säkerställa lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Fråga:

- Beskriv hur principerna efterlevs.

Rätt 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?
- Är information lätt att läsa och ta till sig?
- Använder organisationen standardiserade blanketter för att informera om personuppgiftsbehandling? I så fall, hur

används de? Bifoga en inventeringslista över befintliga blanketter.
- Ingår uppdatering av blanketter i plan för GDPR-arbete?

Samtycke och 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.

Fråga:

- 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?

Rätt 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.

Frågor:

- Finns det fastställda rutiner för hur begäran om registerutdrag bör hanteras?
- Har ni fått begäran om registerutdrag? Hur har ni hanterat denna?
- Hur säkerställs det att den registrerade får svar inom rimlig tid?
- Har det uppstått svårigheter vid hanteringen av begäran om registerutdrag? Behöver rutinen ändras, på vilket sätt?
- Säkerställs att identifieringen är tillräcklig?

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 behandling, särskilt sådan som använder ny teknik och med hänsyn till behandlingens art, omfattning, sammanhang och syfte, sannolikt medför en hög risk för fysiska personers rättigheter och friheter, ska PUA före behandlingens påbörjande genomföra en konsekvensbedömning av den planerade behandlingen ur ett dataskyddsperspektiv.

PUA ska säkerställa att enskildas rättigheter och friheter skyddas vid särskilt riskfyllda personuppgiftsbehandlingar, att behandlingen sker lagligt och att detta kan visas.

Vid genomförandet av en konsekvensbedömning avseende dataskydd ska PUA rådfråga dataskyddsombudet.

Frågor:

- Har det genomförts konsekvensbedömningar för de mest kritiska processer?
- Finns tydliga rutiner för att enkelt kunna genomföra en konsekvensbedömning avseende dataskydd?

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 2026s tillsyn.

År 3 – 2028

Granskningen avser:

- Rätt till rättelse och rätt till radering
- Rätt till dataportabilitet
- Register över behandlingar

- Personuppgiftsincidenter
- Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal
- Personuppgiftsbiträden och underbiträdens arbete med GDPR
- Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet
- Dataskyddsombudets uppföljning av fjolårets tillsyn

Rätt till rättelse och rätt till radering

Målet är att:

- Den registrerade har rätt till både rättelse och radering av information, vilket medför skyldighet för organisationen och kräver att den har kunskap och rutiner för att tillgodose dessa rättigheter.

Beskrivning av krav

Den registrerades rättigheter regleras i GDPR och omfattar rättigheter i lagstöd som den registrerade kan åberopa gentemot PUA, inklusive skydd mot vissa automatiserade individuella beslutsfattanden och profilering. Rätten till rättelse innebär att den registrerade, under vissa omständigheter, har rätt att få felaktiga personuppgifter rättade och ofullständiga uppgifter kompletterade. Organisationen måste göra det möjligt för registrerade att enkelt och kostnadsfritt uppdatera sina personuppgifter utan onödigt dröjsmål. Rätten till radering, eller ”rätten att bli bortglömd”, innebär att den registrerade, under vissa förutsättningar, har rätt att få sina personuppgifter raderade. Personuppgifter behöver dock inte raderas om de är nödvändiga för att fullfölja avtal med den registrerade eller om lagar, förordningar eller andra offentliga föreskrifter föreskriver annat. Varje registrerad ska informeras när deras personuppgifter raderas eller anonymiseras.

Fråga

- Finns det fastställda rutiner för hur sådana begäran bör hanteras?

Rätt till dataportabilitet

Målet är att:

- PUA har möjlighet, kunskap och rutiner för att kunna flytta personuppgifter till en annan PUA.

Beskrivning av krav

Om den registrerade har samtyckt till att lämna sina personuppgifter till PUA eller om hen lämnat uppgifterna med anledning av ett avtal kan den registrerade begära att få ut uppgifterna. Rätten till dataportabilitet innebär dels en rätt för den registrerade att få tillgång till personuppgifter, dels en rätt att överföra personuppgifter från en personuppgiftsansvarig till en annan. För att bestämmelserna om dataportabilitet ska bli tillämpliga krävs att behandlingen baseras antingen på samtycke eller ett avtal där den registrerade är avtalspart.

Fråga:

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

Register över personuppgiftsbehandlingar

Målet är att:

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

Beskrivning av krav

PUA är skyldig 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?

Personuppgiftsincidenter

Målet är att:

- Personuppgiftsincidenter dokumenteras och följs upp systematiskt, och incidenter 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?
- Har PUA haft incidenter som rapporterats till IMY?

Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal

Målet är att:

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

Beskrivning av krav

PUA och personuppgiftsbiträden ska upprätta ett så kallat personuppgiftsbiträdesavtal om biträdet behandlar personuppgifter för PUA:s räkning. GDPR räknar upp vad ett sådant biträdesavtal ska innehålla.

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

Frågor:

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

Personuppgiftsbiträden och underbiträdens arbete med GDPR

Målet är att:

- 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?

Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet

Målet är att:

- Organisationens system är säkra och lagliga, med tekniska möjligheter att begränsa åtkomst, följa upp spårbarhet och skydda känslig information, exempelvis genom kryptering och flerfaktorsautentisering. Det finns även rutiner för tilldelning och avslutande av behörigheter vid anställning, tjänstebytte eller avslut av tjänst.
- Tekniska och organisatoriska säkerhetsåtgärder samt ledningssystem för informationssäkerhet ses över kontinuerligt och genomgår ständiga förbättringar.

Beskrivning av krav

Enligt GDPR ska personuppgifterna 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 personuppgiftsansvarige ska även se över åtgärderna 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 behandlingsystemen 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.

Frågor:

- Finns rutiner för tilldelning och avslutande av behörigheter i samband med anställning, avslutande av tjänst/byte av tjänst?
- Ger verksamhetssystemen möjlighet att begränsa behörigheten?
- 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.

Fråga:

- Beskriv vilka åtgärder som har vidtagits och vilka åtgärder som kvarstår efter 2026s tillsyn.

År 4 – 2029

Granskningen avser:

- Dataskyddsorganisation
- Utbildning, medvetenhet och främjande av dataskyddskultur
- Kontinuerlig Förbättring
- Rätt till behandlingsbegränsning

- Rätt till dataportabilitet
- Rätt till att invända mot behandling
- Rättigheter vid automatiskt beslutsfattande
- Dataskyddsombudets uppföljning av fjolårets tillsyn

Dataskyddsorganisation

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 systematisk och metodisk dataskyddsarbete görs lämpligast i en dataskyddsorganisation. Detta hänger också ihop med PUA:s ansvarsskyldighet att visa hur de följer dataskyddsförordningen.

Fråga:

- Har ni en dokumenterad, beslutad dataskyddsorganisation, med rollbeskrivning, ansvar och avsatt tid för medverkande personer?

Utbildning, medvetenhet och främjande av dataskyddskultur

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?

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 till dataportabilitet

Målet är att:

- PUA har möjlighet, kunskap och rutiner för att kunna flytta personuppgifter till en annan PUA.

Beskrivning av krav

Om den registrerade har samtyckt till att lämna sina personuppgifter till PUA eller om hen lämnat uppgifterna med anledning av ett avtal kan den registrerade begära att få ut uppgifterna. Rätten till dataportabilitet innebär dels en rätt för den registrerade att få tillgång till personuppgifter, dels en rätt att överföra personuppgifter från en personuppgiftsansvarig till en annan. För att bestämmelserna om dataportabilitet ska bli tillämpliga krävs att behandlingen baseras antingen på samtycke eller ett avtal där den registrerade är avtalspart.

Fråga:

- Finns det fastställda rutiner för hur begäran om dataportabilitet 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?

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 föregående års tillsyn.

År 5 – 2030

Granskningen avser:

- Struktur, rutiner och processer
- Rättslig grund för personuppgiftshantering
- Lagringsminimering och gallring
- Övriga principer
- Rätt till information
- Samtycke och samtyckesprocess
- Rätt till tillgång
- Personuppgiftsincidenter
- Dataskyddsombudets uppföljning av fjolårets tillsyn

Struktur, rutiner och processer

Målet är att:

- Organisationen har ekonomiska och personella resurser för ett systematiskt dataskyddsarbete som är anpassat till mängden och typen av personuppgiftsbehandlingar, där dataskydd är integrerat i verksamheten, dokumenterat och bedrivs på ett systematiskt sätt.

Beskrivning av krav

Dataskyddsförordningen kräver att organisationer genomför och löpande underhåller ett strukturerat dataskyddsarbete. Det innebär bland annat att ta fram dokumentation, besluta om styrdokument, införa processer för dataskydd och säkerställa att medarbetare har tillräcklig kunskap, exempelvis för att kunna identifiera och rapportera personuppgiftsincidenter.

Personuppgiftsansvarig (PUA) ansvarar för att skapa förutsättningar för detta arbete genom att säkerställa resurser, planering samt lämpliga tekniska och organisatoriska åtgärder. Åtgärderna ska anpassas efter behandlingens risker och regelbundet följas upp. För att uppfylla ansvarsskyldigheten enligt GDPR behöver organisationen också ha relevanta styrdokument, rutiner och processer som integrerar dataskydd i verksamhetens ordinarie arbete.

Frågor:

- Finns det en beslutad verksamhetsplan, årsplan eller handlingsplan för organisationens dataskyddsarbete?
- Är organisationens rutiner och processer för dataskydd dokumenterade?
- Hur säkerställs att dataskydd integreras i verksamhetens ordinarie arbete (t.ex. genom styrdokument, rutiner eller utbildning)?

Dataskyddsorganisation

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 systematisk och metodisk dataskyddsarbete görs lämpligast i en dataskyddsorganisation. Detta hänger också ihop med PUA:s ansvarsskyldighet att visa hur de följer dataskyddsförordningen.

Fråga:

- Har ni en dokumenterad, beslutad dataskyddsorganisation, med rollbeskrivning, ansvar och avsatt tid för medverkande personer?

Rättslig grund för personuppgiftsbehandlingar

Målet är att:

- Rättslig grund finns dokumenterad för varje personuppgiftsbehandling.
- Intresseavvägningar är dokumenterade.
- Samtycken är dokumenterade på rätt sätt och kan återtas.

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:

- Dokumenterar och motiverar PUA på ett lämpligt sätt er rättsliga grund för behandling av personuppgifter samt om behandlingen involverar känsliga personuppgifter eller uppgifter om brott?
- Är information om ändamålet med behandlingen och den rättsliga grunden allmänt tillgänglig, lätt att hitta, komma åt och läsa?

Lagringsminimering och gallring

Målet är att:

- Personuppgifter raderas eller avidentifieras för varje personuppgift som inte längre behövs för ändamålet. Undantaget är personuppgifter som måste sparas i enlighet med annan lagstiftning. Gallring ska genomföras för att leva upp till principen om lagringsminimering.

Beskrivning av krav

PUA får spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När personuppgifterna inte längre behövs för ändamålet ska de raderas eller avidentifieras. PUA ska därför införa rutiner för gallring av personuppgifter, till exempel att genomföra regelbundna kontroller eller radering efter viss tid.

I vissa fall måste handlingar som innehåller personuppgifter sparas även efter det att PUA slutat använda dem. Det gäller till exempel bokföring, där bokföringslagen ställer krav på hur länge vissa handlingar ska sparas. Lagra då handlingarna på ett sådant sätt att de inte längre är tillgängliga i den dagliga verksamheten, det vill säga avskilj personuppgifterna.

Det kan också vara tillåtet att lagra personuppgifter när det ursprungliga ändamålet inte längre är aktuellt, om det sker för:

- arkivändamål av allmänt intresse
- vetenskapliga eller historiska forskningsändamål
- statistiska ändamål.

Frågor:

- Fungerar gallring, avskiljning och arkivering?
- Finns beslutade gallringstider?
- Utförs gallring i system och i ostrukturerat material (Outlook, Intranät, Teams) i enlighet med interna styrdokument?

Övriga principer

Målet är att:

- Säkerställa att GDPR efterlevs inom alla principer.

Beskrivning av krav

Ändamålsbegränsning – säkerställa att personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska inte anses vara oförenlig med de ursprungliga ändamålen.

Uppgiftsminimering – säkerställa att personuppgifter är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Riktighet (korrekthet) – säkerställa att personuppgifter är riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Integritet och konfidentialitet – säkerställa lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Fråga:

- Beskriv hur principerna efterlevs.

Rätt 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?
- Är information lätt att läsa och ta till sig?
- Använder organisationen standardiserade blanketter för att informera om personuppgiftsbehandling? I så fall, hur används de? Bifoga en inventeringslista över befintliga blanketter.
- Ingår uppdatering av blanketter i plan för GDPR-arbete?

Samtycke och 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.

Fråga:

- 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?

Rätt 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.

Frågor:

- Finns det fastställda rutiner för hur begäran om registerutdrag bör hanteras?
- Har ni fått begäran om registerutdrag? Hur har ni hanterat denna?
- Hur säkerställs det att den registrerade får svar inom rimlig tid?
- Har det uppstått svårigheter vid hanteringen av begäran om registerutdrag? Behöver rutinen ändras, på vilket sätt?
- Säkerställs att identifieringen är tillräcklig?

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 behandling, särskilt sådan som använder ny teknik och med hänsyn till behandlingens art, omfattning, sammanhang och syfte, sannolikt medför en hög risk för fysiska personers rättigheter och friheter, ska PUA före behandlingens påbörjande genomföra en konsekvensbedömning av den planerade behandlingen ur ett dataskyddsperspektiv.

PUA ska säkerställa att enskildas rättigheter och friheter skyddas vid särskilt riskfyllda personuppgiftsbehandlingar, att behandlingen sker lagligt och att detta kan visas.

Vid genomförandet av en konsekvensbedömning avseende dataskydd ska PUA rådfråga dataskyddsombudet.

Frågor:

- Har det genomförts konsekvensbedömningar för de mest kritiska processer?
- Finns tydliga rutiner för att enkelt kunna genomföra en konsekvensbedömning avseende dataskydd?

Personuppgiftsincidenter

Målet är att:

- Personuppgiftsincidenter dokumenteras och följs upp systematiskt, och incidenter 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?
- 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 2026s tillsyn.