Sundsvalls kommun

Tillsynsplan dataskydd

2023–2027

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Innehåll

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

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 2023–2027 och planen kommer att uppdateras inför varje nytt år.

Granskningen kommer utföras i tre olika nivåer, liten granskning, mellan granskning eller stor granskning. Nivån på granskning baseras på antalet personuppgifter samt hur känsliga personuppgifter som organisationen behandlar.

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. Granskningsarbetets omfattning beror naturligtvis på organisationens verksamhet, antal registrerade (anställda, kunder, medborgare), hur många personuppgifter som behandlas, hur stor andel som är känsliga eller skyddsvärda personuppgifter.

Personuppgiftsansvariga organisationer:

Sundsvall

Organisation	Namn	Typ av granskning
Bolag	Mitthem	Mellangranskning
Bolag	MittSverige Vatten och Avfall AB	Mellangranskning
Bolag	Servanet	Mellangranskning
Bolag	SKIFU AB	Mellangranskning
Bolag	Stadsbacken AB	Liten granskning
Bolag	Sundsvall Timrå Airport	Mellangranskning
Bolag	Sundsvalls Elnät AB	Mellangranskning
Bolag	Sundsvalls Energi AB	Mellangranskning
Bolag	Sundsvalls Hamn AB	Liten granskning
Bolag	Sundsvalls logistikpark AB	Liten granskning
Bolag	Sundsvalls Oljehamn AB	Liten granskning
Förbund	Medelpads räddningsförbund	Mellangranskning
Nämnd	Barn och utbildningsnämnden	Stor granskning

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

Nämnd	Individ och arbetsmarknadsnämnden	Stor granskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Kultur och Fritidsnämnden	Mellangranskning
Nämnd	Lantmäterinämnden	Liten granskning
Nämnd	Miljönämnden	Mellangranskning
Nämnd	Stadsbyggnadsnämnden	Mellangranskning
Nämnd	Valnämnden	Liten granskning
Nämnd	Vård och omsorgsnämnden	Mellangranskning
Nämnd	Överförmyndarnämnden	Liten granskning

Timrå

Organisation	Namn	Typ av granskning
Bolag	Timråbo	Mellangranskning
Nämnd	Barn och utbildningsnämnden	Stor granskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Kultur och tekniknämnden	Stor granskning
Nämnd	Miljö och byggnadsnämnden	Mellangranskning
Nämnd	Socialnämnden	Stor granskning
Nämnd	Valnämnden	Liten granskning

Ånge

Organisation	Namn	Typ av granskning
Bolag	Ånge Energi AB	Mellangranskning
Bolag	Ånge Fastighets och Industri AB	Mellangranskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Myndighetsnämnden	Stor granskning
Nämnd	Valnämnden	Liten granskning

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Tillsynsplan

Utifrån dataskyddsförordningens krav, ett riskbaserat arbetssätt och kunskap om de ingående organisationerna planeras följande tillsynsplan. DSO beslutar i vilken ordning och om eventuellt parallellt utförande av aktiviteter under året ska genomföras.

Sammanställning år 2023–2027

Rubrik	-23	-24	-25	-26	-27
Organisera arbetet/strategi	X				
Rutiner/dokumentation/processer	X				
Utbildning/medvetenhet/följsamhet och kultur	X		X		X
Översyn/kontinuitet/uppföljning				X	
Revidera och förbättra					X
Rättslig grund för personuppgiftshantering		X			X
Lagringsminimering och gallring					X
Övriga principer					X
Rätt till information		X			
Samtycke/samtyckesprocess		X			
Rätt till tillgång		X			
Rätten till rättelse			X		
Rätten till radaring			X		
Rätt till behandlingsbegränsning				X	
Rätt till dataportabilitet				X	
Rätt att invända mot behandling				X	
Rättigheter vid automatiserat beslutsfattande				X	
Register över personuppgiftsbehandlingar	X		X		X
Dataskyddsorganisation	X		X		X
Personuppgiftsincidenter		X		X	
Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal			X		
Personuppgiftsbiträdens och underbiträdens arbete med GDPR			X		
Konsekvensbedömningar		X			X
Personuppgiftsprocesser och tredjelandsöverföringar		X			
Tekniska/organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet			X		
Dataskyddsombudet	X			X	
Automatiserade beslut/profilering				X	
Tillsyn och följsamhet					X

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Genomförande och redovisning

För att genomföra granskningsarbetet kommer DSO att behöva ta del av olika dokument samt att vissa resurser hos respektive PUA behövs för intervjuer och fördjupade granskningar av GDPR-arbetet. Granskningen kan som exempel utgå från enkäter, intervjuer, styrdokument och stickprovskontroller.

Stickprov kommer att göras på e-tjänster och blanketter för att se att rätt information till de registrerade finns där. Stickprov kommer även att göras för att se att erforderliga personuppgiftsbiträdesavtal blivit tecknade. Stickprov kommer också gälla verksamhetssystem.

Varje område har ett mål, beskrivning av krav och underlag med frågeställningar beroende på om det är en liten granskning, mellangranskning eller stor granskning.

Resultatet av granskningen lämnas i en skriftlig rapport med rekommendationer till PUA:s högsta förvaltningsnivå. För mellangranskning och stor granskning kan DSO komma att genomföra muntlig rapportering.

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

År 1 - 2023, perioden september-december

Granskningen avser:

- Organisera arbetet/strategi
- Rutiner/dokumentation/processer
- Utbildning/medvetenhet/följsamhet och kultur
- Register över behandlingar
- Dataskyddsorganisation
- Dataskyddsombud

Organisera arbetet/strategi

Målet är att:

- Organisationen har ekonomiska och personella resurser för ett systematiskt dataskyddsarbete anpassade till mängden och typen av personuppgiftsbehandlingar.

Beskrivning av krav

Hela dataskyddsförordningen förutsätter att en rad arbetsinsatser behöver genomföras och därefter underhållas. Arbetsinsatserna innebär bland annat upprättande av nödvändig dokumentation, besluta om nödvändiga styrdokument, införande av processer relaterade till GDPR och öka kunskapsnivån inom organisationen. Exempelvis om anställda inte vet vad en personuppgiftsincident är kan en sådan heller inte anmälas.

PUA måste därför skapa övergripande förutsättningar för att dataskyddarbetet ska kunna genomföras.

Underlag, exempelfrågor

- Finns det en beslutad budget och/eller verksamhetsplan för dataskyddsarbetet som gäller för år 2023?
- Redovisas dataskyddsarbetet till ledningen?
- Finns en beslutad verksamhetsplan för dataskyddsarbetet?

Rutiner/dokumentation/processer

Målet är att:

- Dataskydd är integrerat i verksamheten, dokumenterat och att dataskyddsarbetet sker systematiskt.

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Beskrivning av krav

PUA har allmänna skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingar utförs i enlighet med dataskyddsförordning. Vilka åtgärderna som är tillämpliga ska avgöras med beaktande av behandlingens art, omfattning sammanhang och ändamål samt risker för fysiska personers fri- och rättigheter. Ytterligare ska dessa åtgärder ses över och uppdateras vid behov.

Vidare förutsätts att relevanta styrdokument finns på plats för att PUA ska kunna säkerställa att förordningen följs i enlighet med ansvarsskyldigheten som enligt GDPR krävs av PUA.

PUA ska därför ta fram skriftliga rutiner och processer kopplat till dataskyddet och dokumentera resultatet.

Underlag, exempelfrågor

- Arbetar er organisation processbaserat generellt? Motivera ditt svar.
- Arbetar er organisation processbaserat med dataskyddet? Motivera ditt svar.
- Arbetar er organisation processbaserat generellt? Motivera ditt svar.

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.

Underlag, exempelfrågor

- I vilken utsträckning och form får nyanställda utbildning/information om GDPR?

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

- Finns det dokumentation över vilken utbildning som anställda har fått om GDPR?
- När senast genomfördes utbildning?

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.

Underlag, exempelfrågor

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

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.

Underlag, exempelfrågor

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

Dataskyddsombud

Målet är att:

- Det ska finnas ett utsett oberoende dataskyddsombud som rapporterar till högsta förvaltningsnivå.

Beskrivning av krav

Enligt GDPR är det obligatoriskt för myndigheter och andra offentliga organ att utse ett dataskyddsombud. PUA ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten. PUA ska även se till att tillhandahålla DSO de resurser som krävs för att dataskyddsarbete ska fungera på ett bra sätt.

Underlag, exempelfrågor

- Förväntas dataskyddsombudet regelbundet rapportera till organisationens högsta ledningsnivå? Om så är fallet, hur ofta (på årsbasis)?
- Har er organisation offentliggjort dataskyddsombudets kontaktuppgifter och meddelat dessa till IMY? Dataskyddssamordnare ska kontrollera att kontaktuppgifterna till dataskyddsombudet går att hitta på officiell webbplats samt intranät. Komplettera svaret med dessa uppgifter samt med datum för kontrollen.

Intervju av DSO

Då detta område även omfattar DSO:s egna arbete rekommenderas att en oberoende person intervjuar DSO. Resultatet av intervjun bör delges PUA i årsrapporten.

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

År 2 – 2024

Granskningen avser:

- Rättslig grund för personuppgiftsbehandlingar
- Rätten till information
- Samtycken/samtyckesprocessen
- Rätten till tillgång
- Personuppgiftsincidenter
- Konsekvensbedömningar
- Personuppgiftsprocesser och tredjelandsöverföringar

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).

Underlag, exempelfrågor

- 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?

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

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.

Underlag, exempelfrågor

- Finns informationen på alla ställen där personuppgifter samlas in?
- Är information lätt att läsa och ta till sig?
- Har blanketter uppdaterats och information om GDPR tillförts (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.

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

Underlag, exempelfrågor

- 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.

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.

Underlag, exempelfrågor

- 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.

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

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.

Underlag, exempelfrågor

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

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.

Underlag, exempelfrågor

- Har det genomförts någon konsekvensbedömning?
- Hur har de genomförts, i vilket system, i pappersform?
- Finns tydliga rutiner för att enkelt kunna genomföra en konsekvensbedömning avseende dataskydd?

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

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. Arbete med kartläggning och säkerställa att organisationen kan hantera kraven är nödvändigt för att kunna säkerställa skyddsnivån.

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. Samtliga åtgärder ska i sådana fall utgå från regelverket GDPR. 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. Så snart någon personuppgift behandlas i tredjeland, aktualiseras bestämmelserna om tredjelandsöverföring.

Underlag, exempelfrågor

- Finns det leverantörer i tredje land i er verksamhet?
- Hur ser processen ut för tredje landsöverföringar?
- Är verksamheten medveten om tredjelandsöverföringar och vad det innebär?

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

År 3 – 2025

Granskningen avser:

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

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.

Underlag, exempelfrågor

- 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?

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

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 i GDPR och omfattar rättigheter i lagstöd som den registrerade kan åberopa gentemot PUA. Till rättigheterna tillkommer ett skydd mot vissa automatiserade individuella beslutsfattanden samt profilering.

Rätten till rättelse innebär att en registrerad har rätt att, under vissa omständigheter, få rätta felaktiga personuppgifter och komplettera ofullständiga uppgifter. Organisationer måste göra det möjligt för registrerade att enkelt och kostnadsfritt få sina personuppgifter uppdaterade utan onödigt dröjsmål.

Underlag, exempelfrågor

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

Rätten 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

Den registrerades rättigheter regleras i GDPR och omfattar rättigheter i lagstöd som den registrerade kan åberopa gentemot PUA. Till rättigheterna tillkommer ett skydd mot vissa automatiserade individuella beslutsfattanden samt profilering.

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 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.

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

Underlag, exempelfrågor

- 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 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.

Underlag, exempelfrågor

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

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.

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

Underlag, exempelfrågor

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

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.

Underlag, exempelfrågor

- 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 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

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

GDPR. PUA ska följa upp att deras personuppgiftsbiträden och underbiträden efterlever de personuppgiftsbiträdesavtal som har ingåtts och kunna vis att kontroller genomförts.

Underlag, exempelfrågor

- 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:

- Systemen som kommunen använder sig av är säkra och lagliga, det är tekniskt möjligt att begränsa åtkomst, följa upp spårbarhet och skydda känslig information med krypteringar eller flerfaktorsautentiseringar.
- Tekniska och organisatoriska säkerhetsåtgärder ses över kontinuerligt.
- Det finns rutiner för tilldelning och avslutande av behörigheter i samband med anställning, avslutande av tjänst/byte av tjänst.
- Ett ledningssystem för informationssäkerhet är implementerat 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.

Underlag, exempelfrågor

- 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?

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

År 4 – 2026

Granskningen avser:

- Översyn/kontinuitet/uppföljning
- Rätten till behandlingsbegränsning
- Rätten till dataportabilitet
- Rätten till att invända mot behandling
- Rättigheter vid automatiskt beslutsfattande
- Personuppgiftsincidenter
- Dataskyddsombud
- Automatiserade beslut/profilering

Översyn/kontinuitet/uppföljning

Målet är att:

- PUA regelbundet tar del av egna samt av DSO:s identifierade risker och brister i berörd del av organisationen.

Beskrivning av krav

Enligt GDPR ska PUA genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att personuppgiftsbehandlingen utförs i enlighet med förordningen. Dessa åtgärder ska ses över och uppdateras vid behov. PUA ska därför säkerställa att brister och risker i dataskyddarbetet kommuniceras från högsta förvaltningsnivå, till rätt del av organisationen för åtgärd.

Underlag, exempelfrågor

- Hur ofta efterfrågas information från DSO från högsta förvaltningsnivå?
- Vilka risker har under året informerats om från DSO?
- Har Dataskyddssamordnare regelbundet bjudits in till ledningsgrupp?

Rätten 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.

Underlag, exempelfrågor

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

Rätten 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.

Underlag, exempelfrågor

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

Rätten 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.

Underlag, exempelfrågor

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

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Rättigheter vid automatiskt beslutsfattande

Målet är att:

- PUA har möjlighet, kunskap och rutiner för att kunna hantera automatiskt beslutsfattande på rätt sätt.

Beskrivning av krav

Den registrerade har rätt att inte bli föremål för beslut som enbart grundar sig på automatiserad behandling, såsom automatiskt genererade resultat på ansökningar eller bidrag. Det finns dock undantag från regeln, och det är när den registrerade har lämnat sitt samtycke (gäller dock ej särskilda kategorier av personuppgifter) eller när det är nödvändigt för att ingå eller fullgöra ett avtal, alternativt att sådana beslut tillåts enligt lag eller EU-rätten. När beslut fattas automatiskt ska PUA tala om för den registrerade att beslutet är automatiserat, ge hen rätt att få beslutet granskat av en riktig person samt ge möjlighet att bestrida beslutet.

Underlag, exempelfrågor

- Finns det fastställda rutiner för hur Automatiskt beslutsfattande får genomföras?

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.

Underlag, exempelfrågor

- Finns tydliga rutiner för att snabbt och enkelt kunna hantera personuppgiftsincidenter?

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

Dataskyddsombud

Målet är att:

- Det ska finnas ett utsett oberoende Dataskyddsombud som rapporterar till högsta förvaltningsnivå.

Beskrivning av krav

Enligt GDPR är det obligatoriskt för myndigheter och andra offentliga organ att utse ett Dataskyddsombud. PUA ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten. Förordningen ställer också krav på organisationer som utser ett Dataskyddsombud att dataskyddsombudet ska få de resurser som krävs för att dataskyddsarbetet ska fungera på ett bra sätt.

Underlag, exempelfrågor

- Förväntas dataskyddsombudet regelbundet rapportera till organisationens högsta ledningsnivå? Om så är fallet, hur ofta (på årsbasis)?
- Har er organisation offentliggjort dataskyddsombudets kontaktuppgifter och meddelat dessa till IMY? Dataskyddssamordnare ska kontrollera att kontaktuppgifterna till dataskyddsombudet går att hitta på officiell webbplats samt intranät. Komplettera svaret med dessa uppgifter samt med datum för kontrollen.
- Förväntas dataskyddsombudet regelbundet rapportera till organisationens högsta ledningsnivå? Om så är fallet, hur ofta (på årsbasis)?

Automatiserade beslut/profilering

Målet är att:

- Säkerställa att processen för automatiserade beslut/profilering uppfyller sitt krav

Beskrivning av krav

Vissa personuppgiftsansvariga, till exempel banker, skattekontor och sjukhus använder algoritmer för att fatta beslut om dig med hjälp av dina personuppgifter. Det är effektivt för dem, men inte alltid öppet och tydligt för dig som enskild. Sådana beslut kan påverka dig juridiskt eller på annat sätt ha inverkan på din tillvaro.

När beslut fattas automatiskt måste den personuppgiftsansvariga tala om för dig att beslutet är automatiserat, ge dig rätt att få beslutet granskat av en riktig person, ge dig möjlighet att bestrida beslutet.

Kommunstyrelsekontoret 2023-09-04
Dataskyddsombud
Camilla Eriksson

Underlag, exempelfrågor

- Använder man sig av automatiserade beslut i verksamheten?
- Om det används, är processen säkerställd?

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

År 5 – 2027

Granskningen avser:

- Utbildning/medvetenhet/följsamhet och kultur
- Revidera och förbättra
- Rättslig grund för personuppgiftsbehandlingar
- Lagringsminimering och gallring
- Övriga principer
- Register över behandlingar
- Konsekvensbedömningar
- Tillsyn och följsamhet

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.

Underlag, exempelfrågor

- 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?

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

Revidera och förbättra

Målet är att:

- Övergripande säkerställa att PUA har interna regler för att mäta, revidera och förbättra arbetssättet.

Beskrivning av krav

PUA ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med GDPR. Dessa åtgärder ska ses över och uppdateras vid behov. Åtgärderna kan omfatta PUAs genomförande av lämpliga regler för dataskydd och tillämpningen av godkända uppförandekoder eller certifieringsmekanismer som avses i förordningen. Därför bör PUA anta interna regler och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.

För att kunna bli bättre behöver PUA veta hur bra det går idag. Att identifiera verktyg och arbetssätt för att utvärdera dataskyddsarbetet är därför viktigt. En utvärdering av dataskyddsarbetet kan göras genom att mäta sig mot en standard, exempelvis ISO 27701.

Underlag, exempelfrågor

- Hur många genomförda och uppföljda konsekvensbedömningar har skett under året?
- Hur många dataskyddsträffar med ansvariga chefer för att diskutera det pågående arbetet har genomförts under året?
- Med hur många procent har frekvensnivån på inträffade incidenter minskat under året?

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).

Underlag, exempelfrågor

- 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.

Underlag, exempelfrågor

- 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.

Underlag, exempelfrågor

- Beskriv hur principerna efterlevs.

Register över behandlingar

Målet är att:

- 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.

Underlag, exempelfrågor

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

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.

Underlag, exempelfrågor

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

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.

Kommunstyrelsekontoret
Dataskyddsombud
Camilla Eriksson

2023-09-04

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.

Underlag, exempelfrågor

- Har det genomförts någon konsekvensbedömning?
- Hur har de genomförts, i vilket system, i pappersform?
- Finns tydliga rutiner för att enkelt kunna genomföra en konsekvensbedömning avseende dataskydd?

Tillsyn och följsamhet

Målet är att:

- Vid en granskning av tillsynsmyndigheten ska samarbetet med PUA ha fungerat enligt lagens krav

Beskrivning av krav

Personuppgiftsansvariga och personuppgiftsbiträden ska enligt GDPR samarbeta med tillsynsmyndigheten på begäran. Detta sker bland annat genom att ge tillsynsmyndigheten tillgång till personuppgifter, tillträde till lokaler, utrustning och alla andra medel för behandling av personuppgifter.

Underlag, exempelfrågor

- Beskriv hur samarbetet skulle kunna se ut vid en granskning från tillsynsmyndigheten.