GÖTEBORGS REGIONEN

Årskontroll av dataskyddsarbetet 2022

Av Dataskyddsombuden
Malin Ericsson

Innehåll

Inledning/förord

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud, DSO. Denna roll har till uppgift att övervaka verksamhetens integritets och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå. Denna årsrapport är således ett medel för nämnden att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen.
Årsrapporten syftar till att nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten kan ses som en del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Årskontrollen bygger på fasta kontrollpunkter där dataskyddsombuden har ombett respektive nämnds förvaltning eller sektor att beskriva arbetssätt och nuläge. Rapporten presenterar först de inkomna svaren från förvaltningen. Varje svar kompletteras sedan med en kommentar och eventuella rekommendationer från dataskyddsombuden.

Kontrollpunkter

Dataskyddsorganisation

Frågan så som den ställdes till organisationen: *Beskriv verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete. Dataskyddsombuden önskar att verksamheten beskriver och resonerar kring verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt de resurser som tillhandahålls för arbetet. Dataskyddsombuden vill att verksamheten i sina svar resonerar om de anser att organisationen fungerar, om de har tillräckligt med resurser för att proaktivt arbeta med dataskydd, hur organisationen strategiskt arbetar med dataskydd, om det finns rätt kompetens, samt hur dataskyddsorganisationen bidrar till att dataskyddsarbetet är en naturlig del i verksamhetens processer.*

Bifoga: Om möjligt en organisationsskiss som visar dataskyddsorganisationens struktur, och om det finns styrdokument i kommunen som beskriver hur en dataskyddsorganisation ska se ut. Bifoga gärna också om dataskyddsorganisationen har en strategi eller årsplanering för sitt dataskyddsarbete.

Verksamhetens svar:

Dataskyddsorganisation
Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren. Roller som arbetar med informationssäkerhet och IT-säkerhet fungerar som stöd till medarbetare, verksamheter och kommunens ledning att kunna ta ansvaret för informationssäkerheten.

Kommunfullmäktige fastställer övergripande mål och principer för informationssäkerhetsarbetet genom en kommunövergripande informationssäkerhetspolicy. Kommunstyrelsen säkerställer att kommunens arbete med efterlevnad av dataskyddsförordningen sker på ett korrekt och samordnar sätt samt att kommunens informationssäkerhetspolicy efterföljs. För att underlätta för respektive personuppgiftsansvarig att fullgöra sina skyldigheter tar styrelsen fram och uppdaterar mer detaljerade rutiner, mallar och annat underlag. Detta innebär inte någon inskränkning eller begränsning av respektive personuppgiftsansvarigs ansvar.

Utifrån ”Handlingsplan Informationssäkerhet och Dataskydd i Alingsås kommun 2022” har en ny dataskyddsorganisation upprättats inom kommunledningskontoret. Organisationens syfte är att vara kommunens centrala dataskyddssamordnare inom områdena registerförteckning, personuppgiftsbiträdesavtal, tredjelandsöverföringar, personuppgiftsincidenter samt styrning och ledning. Organisationen ska lämna rådgivning till övriga förvaltningar inom dataskyddsområdet.

- Säkerhetschef – har det övergripande ansvaret att leda, utveckla och samordna Alingsås kommuns säkerhetsarbete.

- Informationssäkerhetssamordnare – har det övergripande ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetssamordnare ska arbeta i samråd med säkerhetschefen och övriga ledamöter i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.
- IT-säkerhetssamordnare – har det övergripande ansvaret att säkerställa säkerheten i Alingsås kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Ingår i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.
- Kommunjurist – har det övergripande ansvaret att leda, utveckla och samordna arbetet med hantering av personuppgifter. Ingår i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.

Ansvar inom respektive verksamhet

Kommunstyrelsen och varje nämnd i Alingsås kommun är personuppgiftsansvarige för den personuppgiftsbehandling som sker inom respektive verksamhet. Styrelsen och respektive nämnd är därmed ansvariga för att inom sitt verksamhetsområde se till att gällande dataskyddslagstiftning samt att ”Policy för behandling av personuppgifter” i Alingsås kommun följs. Varje nämnd utser en kontaktperson/GDPR-samordnare som är ansvarig för samordningen av arbetet med personuppgiftshantering på respektive förvaltning. Dessa personer ingår i nätverket Informationssäkerhet och dataskydd som arrangeras av kommunstyrelsen med syfte att samordna arbetet med informationssäkerhet och dataskydd inom kommunen.

- Kontaktperson/GDPR-samordnare för Barn- och ungdomsförvaltningen – ansvarar för att samordna arbetet med informationssäkerhet och dataskydd på Barn- och ungdomsförvaltningen, t.ex. personuppgiftsincidenter, registrerades rättigheter (exempelvis begäran om registerutdrag samt rättelse och radering), registerförteckning, information till registrerade, säkerhetsbedömning av digitala tjänster/appar, personuppgiftsbiträdesavtal. Ingår som förvaltningens representant i nätverket Informationssäkerhet och dataskydd.
- System-/Objektägares ansvar – ansvarar för att objekt efterlever kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.
- Förvaltningschef – ytterst ansvarig för system/objekt inom sin verksamhet. Förvaltningschef kan delegera system-/objektägarskap till annan roll inom sin verksamhet.
- Medarbetare – alla medarbetare inom verksamheten har ett ansvar att följa verksamhetens informationssäkerhetsarbete. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler.

Dataskyddsombud

Dataskyddsombud via samverkansavtal med Göteborgsregionen (GR). Dataskyddsombudet har bland annat till uppgift att informera och ge råd till den personuppgiftsansvarige kring vilka skyldigheter som gäller enligt dataskyddslagstiftning, samt att övervaka efterlevnaden av dataskyddslagstiftningen.

Dataskyddsarbetes organisation i verksamheten
En välfungerande organisation finns. I takt med att organisation och omvärld förändras finns också konstant behov av att roller och ansvarsområden förtydligas och förmedlas i organisationen. Ett kvalitativt arbete med dataskydd är mycket resurskrävande och verksamheterna har en stor andel personuppgiftsbehandlingar. Förvaltningen har allokerat om resurser för att möta ökade krav samtidigt som en del frågor kräver juridisk specialistkompetens som idag saknas i organisationen. De resurser som finns för arbetet med dataskydd används för att arbeta strategiskt utifrån ”Informationssäkerhetspolicy i Alingsås kommun” och tillhörande ”Handlingsplan för informationssäkerhet och dataskyddsarbete”. Det strategiska arbetet sker i huvudsak på förvaltningscentral nivå och innehållet i handlingsplanen verkställs tillsammans med verksamheterna och innefattar bland annat verksamhetsanalys, riskanalys och kontinuitetsplanering. Det genomförs informationsinsatser och det förs en dialog om informationssäkerhet och dataskydd för att verka för att det ska vara en naturlig del av verksamhetens processer sker dels i samtal med rektorer och andra enhetschefer, elevhälsa och administrativ personal men också i samtal med IKTansvarig personal vid varje enhet.
Dataskyddsorganisationen finns beskriven i ”Informationssäkerhetspolicy i Alingsås kommun” som innehåller kommunens långsiktiga målsättning med informationssäkerhetsarbetet och dataskydd. Det årliga arbetet beskrivs inom ramen för ”Handlingsplan för Informationssäkerhet och Dataskydd i Alingsås kommun” som innehåller kommunens beslutade aktiviteter för kommande år med syfte att uppnå fullmäktiges långsiktiga mål. Ny handlingsplan fastställs inför varje år av roller och ansvar inom kommunen gällande arbete med dataskydd.

Kommentar från DSO:

Dataskyddsombudet ser det som positivt att förvaltningen följer den kommungemensamma strukturen och att det centralt inom Barn-och ungdomsförvaltningen finns en grundläggande lokal dataskyddsorganisation där det förvaltningsövergripande dataskyddsarbetet bedrivs. En lokal dataskyddsorganisation är ett nödvändigt komplement till kommunens centrala dataskyddsorganisation och även i förhållande till dataskyddsombuden. Det är även positivt att Barn- och ungdomsnämnden har utsett en GDPR-samordnare som är förvaltningens dataskyddskontakt som ansvarar för att samordna arbetet med informationssäkerhet och dataskydd.

Förvaltningen bör dock resonera i hur den lokala dataskyddsorganisationen kan stärkas och överväga vilka resurser som är rimliga i förhållande till verksamhetens personuppgiftsbehandlingar och risker knutna till dem. Dataskyddsarbetet ska inte ses som ett eget verksamhetsområde utan behöver integreras som ett naturligt inslag i förvaltningens samtliga processer. Förvaltningen hanterar i stor omfattning personuppgifter som bland annat rör barn och bör således ha en rigorös organisation som kan ta ansvar för dataskyddsarbetet i förvaltningens olika uppdrag. Att dataskyddsfrågorna i huvudsak hanteras av en GDPR-samordnare bedöms som relativt optimistiskt om förvaltningen på ett proaktivt sätt ska kunna ta sig an dataskyddsarbetets samtliga delar. Det vore därför önskvärt att förvaltningen utvärderar den egen dataskyddsorganisation och gör en bedömning av om den är ändamålsenlig,

rimlig och tillräcklig i förhållande till förvaltningens uppdrag och de behandlingar som nämnden är ansvarig för. Arbetet bör dokumenteras och förankras. Arbetet bedöms som nödvändigt för att den lokala dataskyddsorganisationen ska få en god förmåga att planera och genomföra insatser för att stärka förvaltningens dataskyddsarbete över tid.

När det gäller att utveckla en lokal dataskyddsorganisation kan det exempelvis handla om att definiera roller och utse digitaliseringsombud i verksamheterna som kan sätta sig in i olika delarna som behöver genomföras för att förvaltningen ska leva upp till dataskyddslagstiftningens krav. Det kan även handla om att ta fram en årsplanering, rutiner eller handläggningsordningar samt att utsedda personer får riktade utbildningsinsatser för det specifika området. Vid behov av utbildningsinsatser samt råd och stöd står dataskyddsombuden till förfogande.

Förvaltningen bör även i samråd med kommunens centrala dataskyddsorganisation förtydliga och klargöra förväntansbilder och ansvarsroller i förhållande till varandra, för att dessa i ska stå i överensstämmelse. I dagsläget kan det vara oklart vilka förväntningar som finns inte minst på den lokala organisationen.

I arbetet med att utvärdera nuvarande organisation för att säkerställa att förvaltningen har tillräckliga resurser på plats bör förvaltningen dokumentera sin dataskyddsorganisation och komplettera med rollbeskrivningar. Här följer ett exempel på hur man kan resonera när man ska se över sin organisation på central respektive lokal nivå.

Beskrivningen bör ge svar på:

1. Vilka kompetenser ingår i den centrala dataskyddsorganisationen som ni inte behöver ta höjd för i den lokala?

2. Vilka kompetenser ska finnas i den lokala dataskyddsorganisationen?

3. Vilka områden ska täckas upp? (dataskydd, arkiv, informationssäkerhet, cybersäkerhet, etc.)

4. Vilka förväntningar kan förvaltningen ställa på den centrala organisationen? (Exempelvis framtagande av mallar, sammanställande av information till registret och informationstexter så dessa ligger på en lagom nivå, Representation vid konsekvensbedömningar, etc.)

5. Vilka förväntningar kan den centrala organisationen ha på den lokala organisationerna/samordnarna? (förmåga att driva frågorna vidare lokalt, göra egna avvägningar och bistå med verksamhetskompetens, etc.)

Här finns mycket att fundera över och de kommentarerna som ges ska ses som förslag på frågor som kan behöva redas ut för att göra organisationen tydligare. Det är viktigt att förvaltningen bygger organisationen efter sina egna förutsättningar och

ambitioner och bör själv definiera vilka frågor man behöver svar på för att uppnå en tydlig organisation.

Det som är viktigt att tänka på när en dataskyddsorganisation tar sin form i en kommun är att ansvaret följer med den som faktiskt är personuppgiftsansvarig. Med det sagt finns det dock inget hinder för att en viss verksamhet inom kommunen utreder och tar fram stödmaterial som andra förvaltningar arbetar efter så länge materialet lever upp till de krav som ställs på respektive personuppgiftsansvarig. Det ansvaret åligger fortsatt respektive personuppgiftsansvarig att slutligt säkerställa.

Därutöver förekommer en del registerlagstiftningar som träffar delar av en kommuns verksamheter. I detta arbete är det bra om den lokala dataskyddsorganisationen bistår med kompetens, som kan ta höjd och gör de bedömningar som är nödvändiga för den specifika verksamheten.

Vad kan organisationen göra

Exakt vad en dataskyddsorganisation ska göra finns inte definierat i GDPR. Det är därför viktigt att kommunen utvärderar och kartlägger det egna behovet. En vanlig känsla när man börjar nysta i detta är att det finns hur mycket som helst att göra och att många frågor hänger ihop och blir väldigt stora. Då är det viktigt att planera och hitta en struktur som kommunen är trygg med. Då blir dataskyddsorganisationen en stabil grund att stå på. Nedan följer exempel på uppgifter som organisationen kan arbeta med. Här kan och bör kommunen också fylla på och utveckla med egna tankar och förväntningar som passar in i kommunens visioner och organisationsform.

1. Registret.

   Central organisation – framtagande och utveckla mall/ system för registret. Korrläsa och bedöma på vilken nivå man väljer i behandlingar. Även agera stöd i val av rättslig grund.

   Lokal organisation – fylla i de personuppgiftsbehandlingar som förekommer i respektive verksamhetsgren. Bekräfta eventuella korrigeringar från centrala organisationen.

   Ett annat sätt skulle vara att den centrala organisationen tar ett helhetsgrepp i upprättandet av registret med hjälp av relevant personal inom respektive sektor/enhet. På så vis får man direkt en jämn nivå i bedömningarna och en organisation som löpande kan revidera registret när behov uppstår.
   Det är viktigt att ha med sig att registret förändras i takt med att kommunen förändras och behöver således ses över med jämna mellanrum.

2. Information till de registrerade.

   Den centrala organisationen kan ha ett ansvar att kontrollera och säkerställa så att informationen till de registrerade är tillräcklig och att det finns en koppling mellan behandlingsregistret och information som går ut till de registrerade.

Den lokala organisationen kan ha ett ansvar att fylla på med verksamhetsspecifik information knuten till behandlingarna med ansvar att täcka upp samtliga lokala processer.

3. Registrerades rättigheter

   Den centrala organisationen kan ha ett ansvar att ha framtagna rutiner och mallar, fastslå lämpliga sökvägar vid registerutdrag så samtliga ansökningar behandlas lika och är tillräckliga etc. Agera stöd vid bedömningar.

   Lokala organisationen kan i sin tur utbilda personal i fastslagna rutiner och mallar beroende på var i organisationen bedömningar och dylikt sker.

   För att hantera registerutdrag har kommunen en bra arbetsgång med ett gediget stödmaterial för att ta omhand när någon vill begära registerutdrag. Kommunen bör dock se över om motsvarande stödmaterial behövs för att tillgodose övriga rättigheter de registrerade har i med dataskyddsförordningen.

4. Incidenter

   Det är bra om den centrala organisationen har en upparbetad rutin för att hantera incidenter. Där man reflekterar över vem som ska bedöma dels allvarlighetsgraden, dels om det ska rapporteras vidare till IMY. Rollbeskrivningarna här är tydliga. Den centrala organisationen bör också följa upp antalet inkomna incidenter även de som inte rapporteras vidare IMY. Detta för att säkerställa så att insatserna som sattes in fått önskade effekter över tid så att liknande incidenter inte orsakas igen och igen.

   Den lokala organisationen kan marknadsföra fastslagna rutiner och uppmuntra personal att rapportera incidenter uppåt i organisationen.

   Dessutom bör kommunen fokusera på att få igång en rapporteringskultur där fler incidenter fångas upp och dokumenteras. Det är högst troligt så att gråzonen är stor. Att få incidenter kommer organisationen till känna behöver nödvändigtvis inte betyda att allt är frid och fröjd utan snarare en indikation på att verksamheter missar att dokumentera och uppmärksamma att de inträffar. Då är det svårt att följa upp och arbeta för att stärka personuppgiftshanteringen.

   Det är också bra att proaktivt förebygga för att klara av att dokumentera incidenter på ett smidigt sätt. Även de av mindre allvarlig karaktär. Incidenter som mer är intressanta att följa upp för statistik och för att få en överblick om hur ofta en specifik typ av incident inträffar. Exempelvis hur många felskickade mail som skickats under en viss period eller behörigheter som är felsatta.

   Dessa ska givetvis alltid bedömas utifrån hur allvarlig varje enskild incident är och hanteras efter konstens alla regler. Men ofta är dessa mindre allvarliga

och bara behöver dokumenteras för lokal uppföljning. Dessa incidenter genererar dock värdefull statistisk information för planeringsarbetet framför allt för att planera och identifiera vilka områden som behöver stärkas och prioriteras. Så det kan finnas ett värde i att fundera hur dessa ska hanteras på ett smidigt sätt.

5. Utbildningar

   Den centrala organisationen kan i samspråk med förvaltningarna bedöma behovet om utbildningar både för den egna centrala organisationen och för de lokala organisationerna. Vilken kunskap är grundläggande för alla medarbetare och vilken kunskap krävs för olika professioner. Ska utbildning ske internt vilket är bra ur många perspektiv så behöver organisationen utvecklas för att klara av det. Ska kommunen istället använda externa utbildare för att utbilda personal så bör man strategiskt planera för det.

   Dataskyddsombuden kan också bistå med utbildningsinsatser inom dataskydd och det gör vi gärna i samspråk med kommunen. Det är dock en sak att ge kurser i dataskydd utifrån vad dataskyddsförordningen och närliggande lagstiftningar säger. Vid sidan av det så finns även en viktig lokal del som behöver finnas med för att utbildningarna ska landa väl och det är de lokala tolkningarna. Om vi samtidigt när vi informerar om vad dataskyddsförordningen säger angående exempelvis registrerades rättigheter också utbildar i de lokala tolkningarna och fastslagna rutiner så får medarbetaren både förklaring kring varför det är viktigt och verktygen och förväntningarna som behövs för att leva upp till kraven.

6. Konsekvensbedömningar

   Den centrala organisationen bör även här vara behjälpliga med rutiner och mallar för vad en konsekvensbedömning ska innehålla. Vidare bör organisationen kunna bidra med representanter som kan agera metodstöd och eventuellt kunna sitta med som samtalsledare för att få ett flyt i konsekvensbedömningarna. Konsekvensbedömningar har en tendens att kännas både tidskrävande och svåra men ju fler man genomför desto smidigare går det. Därför är det en fördel att ha en organisation med medarbetare som har erfarenhet vad en konsekvensbedömning syftar till och vad nyttan av den är.

   Det är också bra att inför en konsekvensbedömning ha med sig ett förarbetat material som fungerar som utgångspunkt för bedömningen. Exempelvis information från registret, processkartor, informationsklassningar, risk och sårbarhetsanalyser, utdrag från handlingar som ingår i processen/behandlingen (dokumenthanteringsplan).

   Det är också bra att fundera på att ha med rätt personer i rummet direkt. Någon som kan processen man tittar på väldigt bra, någon som kan redogöra för de tekniska förutsättningarna, någon som kan vilken juridik som gäller för det man bedömer, etc.

Konsekvensbedömningar är också något som många organisationer släpar efter en hel del med och därför är det viktigt att prioritera efter risk i vilken ände man ska börja med.

På imy.se står det skrivet att en konsekvensbedömning ska genomföras

”Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter måste ni alltid göra en konsekvensbedömning”

Detta gäller på nya behandlingar men också på redan pågående om det saknas. Så det är viktigt att kommunen resonerar hur denna fråga ska tas om hand.

Ett effektivt sätt att ta sig an detta är att föregå konsekvensbedömningarna med så kallade tröskelanaslyser. Alltså en förenklad konsekvensbedömning vars syfte är att ge svar på om det finns behov av att genomföra en konsekvensbedömning eller inte. På detta sätt får man också dokumenterade bedömningar som fungerar som bevis att kommunen har reflekterat över behovet av konsekvensbedömning.

Även vid arbetet med konsekvensbedömningar kan kommunen utnyttja sitt dataskyddsombud som ur sitt perspektiv kan lämna kommentarer och råd utifrån behandlingarna som kommunen planerar att genomföra.

Om det finns kvarvarande risker efter att en konsekvensbedömning genomförts kan det bli aktuellt att blanda in IMY för ett så kallat förhandssamråd. Alltså för att få ett godkännande eller ett förbud från IMY att genomföra tänkt behandling. Här är det också viktigt att reflektera över hur denna beslutsgång ska vara för kommunen. Hur förankras konsekvensbedömningar? Vem ger klartecken för att behandlingen är bedömd och redo för start? Vem beslutar om förhandssamråd? etc.

7. Uppföljningsarbete

Uppföljningsarbete är viktigt för att reda ut både nuläge och för att organisationen ska kunna planera insatser för kommande år och bedöma vilka resurser som kommer att behövas för att utveckla och proaktivt arbeta med dataskydd.

Ett sätt att proaktivt ta sig an dataskyddsarbetet är att börja arbeta med årsplanering. Då är det bra att ta reda på var kommunen står idag, var i arbetet man släpar efter och vilka delar som behöver prioriteras i vilken ordning. Efter det så beslutar kommunen takten och ambitionen i att ta sig ikapp och vilka mål man har med dataskyddsarbetet.

> Denna kartläggning blir också ett effektivt sätt att få med ledningsgrupperna och politiken som strategiskt ska resurs sätta, prioritera, samt ta ansvar för dataskyddsambitionerna.
>
> Ett annat sätt att följa upp dataskyddsarbetet är att bygga in dataskydd som område i befintlig internkontroll vilket Lilla Edet också gjort. Ha med kontrollpunkter som att exempelvis kolla om det finns personuppgiftsbiträdesavtal, Om fastslagna rutiner fungerar etc.
>
> Vidare kan kommunen också resonera kring om det finns värde i att ha återkommande avstämningspunkter som ska redovisas för nämnder och ledningsgrupper. Exempelvis redovisa antal hanterade incidenter, planerade insatser inom området inför nästa år etc. Detta ingår också det i rutinen vilket ses som positivt.

IMY har särskilt lyft fram och uttalat att de ser det som ett generellt problem i Sverige att personuppgiftsansvariga inte har tillräckliga dataskyddsorganisation för att ta sig an dataskyddsfrågorna. Detta i kombination med att de grundläggande principerna inte efterlevs i tillräcklig utsträckning.

Dataskyddsombudet är en aktör som ska verka lite vid sidan av och ge råd i hur man kan resonera samt göra efterlevnadskontroller på relevanta delar av dataskyddsarbetet. Dataskyddsombudet har dock alltid just ett dataskyddsperspektiv i sina bedömningar. Kommunen ska kunna fatta rationella vägval både utifrån dataskyddsombudens råd och egna avvägningar som grundar sig i fler perspektiv (ekonomiska konsekvenser, tidsaspekter etc.) som blir relevanta när beslut om åtgärder krävs. Ofta svåra vägval som sällan har val som är riskfria ur alla perspektiv och därför är det viktigt att kommunen har en etablerad organisation som kan bedöma och ge goda underlag inför beslut. Den ska också ha förmåga att involvera dataskyddsombudet i rimlig utsträckning i frågor som rör dataskyddet.

Alingsås kommun i stort, men också förvaltningen till viss del, har en organisation och personer med uppdrag att arbeta med dataskydd vilket är väldigt bra. Önskvärt hade dock varit att kommunen och förvaltningen mer detaljerat dokumenterar sin organisation inom dataskydd samt tydliggör roller och ansvar. Detta för att öka förståelsen och för att förväntansbilder ska överensstämma så att inget arbete faller mellan stolarna. Det ger också en bättre förutsättning att kompetensutveckla och resurssätta på varje nivå inom kommunen.

En kartläggning behöver också göras för att få en nulägesbild av hur man ligger till i dataskyddsarbetet. Vad gör man bra, vad ligger man efter med, vad bör prioriteras och i vilken takt. En bra utgångspunkt kan vara att kika på de grundläggande principerna i artikel 5 GDPR som på många sätt beskriver dataskyddsförordningens krav på en övergripande nivå och som kan användas som mätvärde för att kontrollera hur man ligger till i ljuset av de formuleringarna. Därefter kan man ta fram med en årsplanering för att proaktivt ta sig an dataskyddsförordningens utmaningar. Arbeta med de delar som man släpar efter i och planera utifrån var man identifierar störst risker.

Rekommendationer från DSO:

- Upprätta en dokumenterad arbetsordning för den lokala dataskyddsorganisationen samt definiera roller och ansvar.
- Genomföra en kartläggning över sitt nuläge för att ringa in förvaltningens behov av organisation inom området och ta fram dokumenterade strategier och visioner.
- Utifrån risk bedöma, prioritera och planera för rimliga insatser genom en dokumenterad årsplanering.

Behandlingsregister och Informationsskyldigheten

Under denna punkt önskar dataskyddsombuden att verksamheten redovisar hur nämndens behandlingsregister ser ut både i egenskap av personuppgiftsansvarig men också i egenskap som personuppgiftsbiträde. Dessutom önskar dataskyddsombuden att verksamheten beskriver sitt bedömda nuläge och hur många av verksamhetens behandlingar som i dagsläget bedöms finns dokumenterade. Dataskyddsombuden önskar också en beskrivning hur verksamheten arbetar i val av rättslig grund samt en motivering kring när den rättsliga grunden samtycke används för personuppgiftsbehandling och de överväganden som gjorts kring användandet av den rättsliga grunden i verksamheten.

Under denna punkt önskar dataskyddsombuden också få en beskrivning om hur verksamheten har arbetat med informationsskyldigheten i allmänhet. Av beskrivningen bör framgå om det huvudsakligen handlar om information när den enskilde själv har lämnat informationen (art. 13 GDPR) och i vilken omfattning som information sker utifrån att förvaltningen fått informationen från någon annan än den enskilde själv (art. 14 GDPR)

Bifoga kopia på registerförteckning som upprättats av nämnden som personuppgiftsansvarig och även det register som ska föras om nämnden som personuppgiftsbiträde. En eller flera informationstexter om behandling av personuppgifter som gått ut till de registrerade rörande någon/några av de behandlingar verksamheten har upprättade i sitt behandlingsregister.

Verksamhetens svar:

Barn- och ungdomsnämnden registerförteckning bifogas. Barn- och ungdomsnämnden har inga behandlingar i dagsläget där nämnden är biträde. Samtliga personuppgiftsbehandlingar som idag sker i digitala system/tjänster finns redovisade i behandlingsregistret.

Utgångspunkten är att personuppgiftsbehandlingar inte ska förekomma om rättsligt stöd saknas. Personuppgiftsbehandlingar inom verksamheten bedöms vara nödvändiga i syfte att genomföra uppdraget att tillhandahålla och bedriva utbildning och annan pedagogisk verksamhet av hög kvalitet i enlighet med skollag och övriga författningar. Exempel på sådana behandlingar är mottagande

av barn och elever och erbjudande av plats i förskola och skola, administrativa ändamål för att kunna planera, genomföra och följa upp elevernas utbildning, registrering av närvaro och frånvaro, dokumentation inför utvecklingssamtal och vid upprättande av individuella studieplaner, dokumentation av olika typer av utredningar, t.ex. om särskilt stöd och i undervisningen genom användandet av t.ex. en digital lärplattform, fortlöpande informera vårdnadshavare om elevens utveckling. Dessa personuppgiftsbehandlingar sker med stöd av den rättsliga grunden uppgift av allmänt intresse. När det gäller åtgärder som vidtas med stöd av skollagen, t.ex. beslut om betyg och beslut om särskilt stöd görs personuppgiftsbehandlingar med stöd av den rättsliga grunden myndighetsutövning. Samtycke används som rättslig grund för personuppgiftsbehandlingar som omfattar foto- film- och ljudupptagning som sker utanför skolans och förskolans ordinarie uppdrag, där lagstöd allmänintresse saknas för personuppgiftsbehandlingen. I dessa fall är syftet annat än pedagogiskt arbete. Det kan exempelvis vara att informera eller att marknadsföra verksamheten.

Särskilda överväganden görs vid behandling av känsliga uppgifter inom ramen för elevhälsoarbetet utifrån Skollagen 2 kap , 25-28 §§ , OSL 23 kap § 1-5, kap 4 § 3. Allmänt intresse utgör rättslig grund för behandlingen samt 26 a kap. skollagen, att känsliga personuppgifter om hälsa ska få behandlas med stöd av artikel 9.2 g GDPR om det är nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Undantagna är personuppgiftsbehandlingar som sker i elevhälsan och som utförs inom hälso- och sjukvården. Sådan personuppgiftsbehandling omfattas i stället av bl.a. patientdatalagens (2008:355) bestämmelser. Det innebär att hälso- och sjukvårdspersonal inom elevhälsan som är skyldig att föra patientjournal och behandla personuppgifter enligt patientdatalagens bestämmelser även fortsättningsvis tillämpar den lagen med tillhörande föreskrifter.

Arbete med informationsskyldighet
Information till de registrerade sker på olika sätt beroende på kontaktväg. Standardhänvisningar finns på Alingsås kommuns hemsida1 vilka också finns hänvisning till i Barn- och ungdomsförvaltningens portal (Arena för lärande) för kommunikation och tillgång till digitala tjänster. I förvaltningens e-tjänster finns information till registrerade anpassade efter respektive behandling. Bifogat finns exempel på information till registrerade i samband med ansökan till grundsärskola samt vid ändring om vistelsetid i förskola.

https://www.alingsas.se/kommun-och-politik/diarium-och-arkiv/sa-hanterar-vi-dina-personuppgifter/

Kommentar från DSO:

Skyldigheten att föra ett register över sina personuppgiftsbehandlingar är en väsentlig del i dataskyddsarbetet. Det är här förvaltningen ska beskriva sina behandlingar och motivera varför de är nödvändiga. Det är också utifrån

behandlingarna i detta register man sedan informerar de registrerade. Dessutom bör förvaltningen utgå från dessa behandlingar när man gör sina eventuella konsekvensbedömningar. GDPR listar ett antal punkter som behandlingsregistret ska ge svar på. IMY har på sin hemsida en bra checklista för att säkerställa att dessa punkter finns med.

- Namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvarigas företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Det är viktigt att primärt säkerställa att alla dessa punkter finns med i registret. Sedan kan man med fördel lägga till fler punkter som ytterligare beskriver behandlingen och vilka skyddsåtgärder man vidtagit i förhållande till varje enskild behandling.

Dataskyddsombudet har inte haft möjlighet att titta närmare på förvaltningens behandlingsregister då något sådant inte fanns bifogat. Nämnas bör att det är vanligt förekommandematt man blandar perspektiv eller listar IT-system som enskilda behandlingar. Så länge man kan svara på de tidigare nämnda punkterna så ”går” det att upprätta ett register utifrån olika perspektiv. Det är dock enklare att förstå och dra nytta av sitt behandlingsregister om det utgår från behandlingar alltså utifrån sina myndighetsuppdrag. Det är också det som är grundtanken i GDPR. Här bör förvaltningen utgå från de myndighetsuppdrag som förvaltningen ansvarar för och formulera sina behandlingar utifrån dem.

Valet av rättslig grund kopplat till en behandling är ett bra exempel på detta. Ett system har ju aldrig ett självändamål för förvaltningen utan är ett stöd i en eller flera processer kommunen har. Exempelvis är ett ärendehanteringssystem ett hjälpmedel för att lagra och hålla ordning på handlingar exempelvis som led i en behandling som skulle kunna heta ”beslut om betyg”. Sedan kanske systemet är lämpligt för att hantera flera olika typer av ärenden och då kan man för varje enskilt uppdrag fylla i registret under respektive behandling vilka systemstöd som används för att nå målet med respektive uppdrag som förvaltningen har. Har man systemet listat som en egen behandling (så som förvaltningen har i bifogat register för vissa behandlingar) blir det mer komplicerat att få en klar bild för vilka ärenden som systemet är till för. I stället bör förvaltningen överväga att utgå

från sina processer som oftast utgår från uppdrag som vilar på kommunen antingen utifrån kommunallagen, Offentlighet och sekretesslagen eller någon speciallagstiftning. Alternativt så utgår de från politiska uppdrag. Dessa uppdrag/behandlingar är tydliga exempel på när förvaltningen ska ange den rättsliga grunden allmänt intresse eller myndighetsutövning. Har man dock angivit ett system som en behandling och som ofta förekommer i många processer blir det mycket mer komplicerat att ange rätt rättslig grund. Istället bör förvaltningen markera de systemstöd som förekommer som stöd för varje enskilt uppdrag/behandling man utför och med stöd av uppdragsbeskrivningen och målet med uppdraget bedöma om systemet är lämpligt och rimligt i förhållande till det. Med ett väl dokumenterat register så kommer förvaltningen uppleva att det är mycket enklare att ta sig an sitt dataskyddsarbete, få koll och kontroll över varför man gör som man gör och säkerställa så man tar omhand samtliga delar.

Informationsskyldigheten blir nästa steg och har man ett väl formulerat behandlingsregister utifrån sina processer/uppdrag så blir det enkelt att kontrollera så man har informationstexter kopplade till varje behandling man utför. Informationen som angivits i behandlingsregistret kan allt som oftast då också återanvändas i informationen ihop med övriga punkter som en informationstext ska innehålla. Det är viktigt att förvaltningen tar fram informationstexter som redovisar samtliga behandlingar man har listat i sitt behandlingsregister och att dessa tillgängliggörs på i ett forum så de når de registrerade helst före en behandling påbörjas. IMY har på sin hemsida många bra tips hur denna skyldighet ska efterlevas. EDPB har också tagit fram en riktlinje kopplad just till denna skyldighet som är läsvärd inför detta arbete.

Rekommendationer från DSO:

- Se över registret och överväg att omarbeta det om det förhåller sig så att det utgår från era IT-system och inte processer/uppdrag som rekommenderas. Uppdrag och ändamålsbeskrivning återfinns främst i för verksamheten tillämplig lagstiftning men även beslut och avtal.
- Koppla informationstexter till de registrerade till samtliga av era behandlingar. Var noga med att informationstexten ger information och tillgängliggörs i enlighet med artikel 13 och 14 GDPR.

Personuppgiftsincidenter

Beskriv verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier.

Beskriv också verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Beskriv också hur verksamheten lever upp till dokumentationsskyldigheten, att alla inträffade personuppgiftsincidenter dokumenteras.

Dataskyddsombuden önskar också en redogörelse kring hur verksamheten arbetar för att uppmärksamma sina anställda om deras viktiga roll att larma vid misstänkt personuppgiftsincident och om de känner till hur de ska agera vid misstanke.

Verksamheten bör ha dokumenterade rutiner som ger goda förutsättningar för att upptäcka och utreda personuppgiftsincidenter. (Fundera över om det finns rutiner, var de finns och om de är kända för all personal i verksamheten samt om de har en tydlig rollfördelning över vem som gör vad när en incident upptäcks eller misstänks ha skett. Fundera och argumentera också över om rutinen följer IMY:s rekommendationer?

Bifoga: Rutiner kring arbetet med personuppgiftsincidenthanteringen. Bifoga också antal identifierade incidenter 2022 samt antal av dessa som anmälts till IMY.

Verksamhetens svar:

Alingsås kommuns rutin för hantering av personuppgiftsincidenter 2 finns bifogad och rutinen är framtagen av Kommunledningskontoret och gäller för samtliga nämnder/styrelser och vänder sig till alla medarbetare och chefer i kommunen. Rutinen ska ses över årligen och vid behov revideras av kommunledningskontoret.

Rutinen finns publicerad på kommunens intranät Kommunportalen tillsammans med länk till den e-tjänst som används inom kommunen för att anmäla en personuppgiftsincident.

Barn- och ungdomsförvaltningen har en kontaktperson/GDPR-samordnare som tar emot anmälan av personuppgiftsincidenter och samordnar arbetet utifrån den rutin som kommunledningskontoret tagit fram samt ger råd och stöd till verksamheten. Personuppgiftsansvarig delegerar till GDPR-samordnare att bedöma om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten.

Dataskyddsombud finns tillgänglig för konsultation avseende denna rutins alla delar men beslut fattas alltid av personuppgiftsansvarig själv.

<u>Anmälan och rapportering vid en personuppgiftsincident (utdrag ur rutinen)</u>
1. Den anställde som själv upptäcker en potentiell incident eller får kännedom om en incident från ett personuppgiftsbiträde kontaktar omedelbart sin närmaste chef.
2. Ansvarig chef och den anställde genomför en första kartläggning av incidenten. Därefter fylls kommunens e-tjänst för anmälan av personuppgiftsincidenter i. Detta sker vanligtvis i samråd med GDPR-samordnare. Anmälan skickas per automatik till Barn- och ungdomsförvaltningens e-postlåda för hantering och utredning samt diarieföring. En kopia skickas till kommunledningskontoret i statistik- och sammanställningssyfte. Anmälan innehåller en beskrivning av:

a. när incidenten upptäcktes
b. händelseförlopp, plats, inblandade program, system och tjänster etc.
c. vad som gjorts för att åtgärda eller mildra effekterna av incidenten
d. vilken typ av incident som har inträffat (t.ex. obehörigt röjande, förlust, ändring).
e. vilka personuppgifter som berörs av incidenten samt vilka kategorier av registrerade som berörs och hur många

f. vilka konsekvenser incidenten kan få
g. bedömning om incidenten ska anmälas till IMY
h. bedömning om de registrerade behöver informeras.

3. GDPR-samordnare bedömer om det är fråga om en personuppgiftsincident och om den ska anmälas till Integritetsskyddsmyndigheten. Samordnaren genomför eventuell anmälan inom 72 timmar från att incidenten blivit känd. Diarienumret från ärendet i diariesystemet (Platina) anges som referensnummer vid anmälan. Diarieföring av själva anmälningen ska också ske hos den personuppgiftsansvarige. Delegationsbeslut ska upprättas för information till ansvarig nämnd. Dataskyddsombud finns att konsultera om ett sådant behov finns.
4. GDPR-samordnare gör bedömningen ifall de registrerade behöver informeras. Om de registrerade behöver informeras så tar ansvarig chef fram en informationsplan och ser till att den verkställs.
5. GDPR-samordnare initierar att ansvarig chef, vid behov i samråd med andra som kan bidra med bedömningen, gör en utredning om incidenten samt inkluderar en plan för att förhindra/minska risken för att liknande händelser sker igen. Utredningen med tillhörande plan för att förhindra/minska risken att liknande händelser sker igen diarieförs tillsammans med övrig dokumentation om incidenten i Platina. i ärendet. Bifogat finns den kommungemensamma utredningsmallen3 som används för utredning och analys av incidenter.

Om flera personuppgiftsansvariga är en del av samma personuppgiftsincident så ska en anmälan per personuppgiftsansvarig upprättas.

Informationsinsatser har genomförts för rektorer och IKT-ansvariga på förskolor/skolor rörande GDPR, dataskyddsfrågor och personuppgiftsincidenter. Som en del av ”Handlingsplan informationssäkerhet och Dataskydd” planeras utbildningsinsatser inom området informationssäkerhet och dataskydd för samtliga anställda.

Rutin för att bedöma incidenter
Om en inträffad händelse bedöms att den ska anmälas till Integritetsskyddsmyndigheten, (IMY), så ska detta ske inom 72 timmar från den tidpunkt som den inträffade. Därför är det viktigt att den interna hanteringen och rapporteringen sker skyndsamt och i nära anslutning till att händelsen upptäcks. Avväganden rörande anmälan till tillsynsmyndigheten (IMY) görs utifrån IMYs riktlinjer ”Riktlinje om anmälan av personuppgiftsincidenter”, och vid behov i samråd med dataskyddsombudet.

Utifrån aktuellt nuläge i verksamheten rörande kompetens för dataskydd är bedömningen att det finns förutsättningar för att identifiera och utreda personuppgiftsincidenter. Samtliga systemansvariga för de digitala system som används för behandling av uppgifter samt Nyckelpersoner och chefer har god kunskap om personuppgiftshantering och tillvägagångssätt vid eventuell incident. Förvaltningen har identifierat behov av ytterligare kompetenshöjande insatser som riktar sig till samtliga i organisationen för att höja den generella kompetensen. Behov finns även inom den kommunala organisationen vad gäller förtydligande av roller och ansvar för kommungemensamma system.

Under 2022 har sex personuppgiftsincidenter identifierats. Inga av dessa har bedömts vara föremål för anmälan till IMY.

alfresco.alingsas.se

alfresco.alingsas.se

Kommentar från DSO:

Dataskyddsombudet anser att kommunen har kommit långt i sitt arbete med att hantera personuppgiftsincidenter. Det är positivt att det finns en kommungemensam centrala process med e-tjänst och rutin för hantering av incidenter och att den är känd av verksamheten. Att ha upprättade rutiner och dokumenterade arbetssätt är en väsentlig del för att ha en god förmåga att bedöma och hantera incidenter inom den 72 timmarsgräns som stadgas i GDPR.

Uppfattningen är att förvaltningen arbetar aktivt med information kring incidentrapportering. Att endast 6 incidenter har uppmärksammats är dock något lågt och förvaltningen bör ställa sig frågan varför det förhåller sig så. Att ett fåtal incidenter upptäcks behöver inte innebära att det inte förekommer fler utan kan i stället vara ett tecken på att de incidenter som inträffar ej kommer dataskyddsorganisationen till känna, vilket är allvarligt. Av de incidenter som hanterats visar dock förvaltningen förmåga i att hantera det inträffade. Att man sedan valt att inte anmälan någon av incidenterna till IMY, manar även det till eftertanke. Dataskyddsombudets slutsats är att det mest troligt föreligger ett mörkertal av personuppgiftsincidenter och att det kan finnas behov av att utbilda anställda i att förstå vad en incident är. Vid behov kan även dataskyddsombuden bistå med utbildningsinsatser inom området. Om utbildning sedan kompletteras med att anställda ges möjlighet att arbeta enligt kommunens rutin kommer troligtvis fler incidenter att upptäckas. Att identifiera, bedöma och anmäla incidenter är ett friskhetstecken och bör uppmuntras. Det är en av grunderna för att utvärdera var i organisationen det förekommer störst risker och var det kan finnas behov av insatser. Ett annat sätt att identifiera incidenter är att låta systemen sköta jobbet i de fall detta är möjligt. Här kan förvaltningen kontrollera med leverantörer om deras IT-lösningar har en funktion som kan signalera när systemet upptäcker avvikelser. Detta kan vara ett sätt att påminna anställda om att se över det inträffade för att identifiera en eventuell incident. Förvaltningen kan i ett nästa steg fundera kring en uppföljningsmodell där man följer upp incidenter och de åtgärder som vidtagits för att utvärdera insatsen och effekterna.

Rekommendationer från DSO:

- Analysera anledningen till att endast 6 incidenter identifierats och att ingen av dessa anmälts till IMY samt utred vilka insatser som kan stärka förmågan inom förvaltningen och utför dessa.
- Bedöm om det finns utbildningsbehov inom förvaltningen och planera för det. Vid behov finns dataskyddsombuden till hands för utbildningsinsatser.

- Ta fram en uppföljningsmodell i syfte att utvärdera insatser och effekterna. Fundera också om ni kan använda de dokumenterade incidenterna för att lokalisera riskområden.

Registrerades rättigheter

Beskriv verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. Beskriv gärna hur verksamheten hanterar en begäran om ett registerutdrag eller radering av personuppgifter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan.

Bifoga: Rutin kopplat till hanteringen av de registrerades rättigheter. Bifoga också om det finns en rutin för att hantera ett tillbakadragande av samtycke. Bifoga också antal ärenden som hanterats under 2022 rörande registrerades rättigheter.

Verksamhetens svar:

Alingsås kommuns rutiner för att hantera begäran om registerutdrag och begäran om rättelse/radering finns bifogade och de är framtagna av Kommunledningskontoret. Registrerade begär registerutdrag samt rättelse/radering via kommungemensamma etjänster som finns tillgängliga på kommunens hemsida. Vad gäller frågan om de registrerades rättigheter, utöver informationsskyldigheten, finns tillgängliga e-tjänster för begäran om registerutdrag och/eller begära rättelse/radering av personuppgifter.

Begäran om registerutdrag alternativt rättelse/ändring skickas per automatik till Barn- och ungdomsförvaltningens e-postlåda för hantering samt diarieföring. GDPR-samordnare på Barn- och ungdomsförvaltningen hanterar och samordnar begäran om registerutdrag och rättelse/radering. När en begäran om registerutdrag inkommer fastställs först vilken roll den registrerade har i verksamheten, såsom vårdnadshavare, elev, personal eftersom all personuppgiftshantering är rollstyrd. Utifrån identifierad roll sammanställs vilka uppgifter som behandlas i vilka system, för vilka syften, hur länge informationen lagras osv. Dessa uppgifter meddelas sedan den registrerade på det sätt som den valt. I vissa verksamhetssystem finns möjlighet för den registrerade att själv ta ut ett registerutdrag (t.ex. närvarosystemet Skola 24). Förekommer inte personen i Barn- och ungdomsförvaltningens system/register, meddelas detta den registrerade skriftligen.

För tillbakadragande av samtycke uppmanas den registrerade att skicka in en anmälan på nytt via Barn- och ungdomsförvaltningens e-tjänst för samtycke (alternativt fylla i blanketten för samtycke) och lämna till aktuell förskola/skola för hantering. Information om hur den registrerade ska gå tillväga vid tillbakadragande av samtycke finns i den e-tjänst och blankett som används för samtycke.

Under 2022 har en begäran om rättelse/radering av personuppgifter inkommit till Barn- och ungdomsförvaltningen.

alfresco.alingsas.se

https://saml02.alingsas.se/my.policy

Kommentar från DSO:

Det är bra att kommunen har en framtagen rutin för att hantera begäran om registerutdrag vilken bör betraktas som den vanligaste aktiva rättigheten de registrerade har, det vill säga att de begär någonting av förvaltningen i enlighet med rättigheterna. Det är också bra att kommunen har en rutin för rättelse och radering av personuppgifter. Det är också positivt att de används av verksamheten. Man ska dock komma ihåg att informationsskyldigheten alltid blir gällande för varje behandling och är en passiv rättighet. Det vill säga att förvaltningen ska göra den registrerade uppmärksammad på att behandling av personuppgifter sker och varför. Det är utifrån denna information som den registrerade har möjlighet att reagera i regel. Förvaltningen bör resonera kring de olika rättigheterna som följer i GDPR, Kapitel III och överväga en rutin som tar höjd för alla eventuella begäranden om att nyttja rättigheter. Detta är ett sätt att visa på att trots att förvaltningen ännu inte fått in särskilt många rättighetsfrågor har en god förmåga att omhänderta dem om och när de kommer.

Rekommendationer från DSO:

- Låt dataskyddsorganisationen sätta sig in i de olika rättigheternas innebörd och ta fram en rutin som täcker alla de olika rättigheternas syften enligt kapitel III, GDPR.

Konsekvensbedömningar

Beskriv verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt arbetsprocessen vid genomförandet av en konsekvensbedömning. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet. Beskriv också verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Bifoga: Om sådan finns, en genomförd konsekvensbedömning och eventuell mall som ska användas i detta arbete.

Verksamhetens svar:

Alingsås kommun har en kommungemensam e-tjänst för konsekvensbedömning av dataskydd. E-tjänsten används i syfte att identifiera huruvida nya eller förändrade personuppgiftshanteringar kräver konsekvensbedömning samt för att genomföra en konsekvensbedömning innehållande en riskanalys, framtagning av rutiner/åtgärder för att bemöta risker och dokumentera hur kraven i

Dataskyddsförordningen uppfylls. Barn- och ungdomsförvaltningen har inte genomfört några konsekvensbedömningar avseende dataskydd enligt Dataskyddsförordningen i dagsläget. Konsekvensbedömning planeras att genomföras för nuvarande behandling av Google Workspace for Education samt inför nya personuppgiftsbehandling som bedöms innebära hög risk för de registrerades fri- och rättigheter.

Kommentar från DSO:

Dataskyddsombudet ser det som positivt att det finns en kommungemensam e-tjänst för konsekvensbedömning och att verksamheten känner till den. Det är också bra att förvaltningen planerar att genomföra konsekvensbedömning på ett nuvarande system. Kravet att ha förmåga att kunna bedöma om behov av och genomförande av konsekvensbedömningar regleras i artikel 35 GDPR. En konsekvensbedömning ska som regel göras inför behandling av personuppgifter men kan också behöva genomföras på behandlingar som redan var pågående då GDPR trädde i kraft. Syftet med en konsekvensbedömning påminner om men ska inte blandas ihop med arbetet med risk och sårbarhetsanalyser inom informationssäkerhetsområdet. Det vill säga att man ska identifiera och lyfta fram risker och tillsätta åtgärder för att eliminera eller minimera riskerna. Till skillnad från informationssäkerhetsarbetet där man kan landa i någon form av riskaptit handlar det här i stället om att analysera behandlingens risker och tillsätta tillräckliga skyddsåtgärder så att behandlingen går att utföra i enlighet med GDPR. Således är konsekvensbedömningsarbetet en viktig pusselbit för att leva upp till ansvarsprincipen. Att kunna visa på att förvaltningen har bedömt sina behandlingar och satt in tillräckliga skyddsåtgärder i syfte att säkerställa att de hanteras i enlighet med dataskyddslagstiftningen. Ibland är det ett krav att göra en konsekvensbedömning över en behandling. På IMY.se finns följande beskrivning kopplat till när en konsekvensbedömning måste finnas.

”Om er behandling faller in under någon av nedanstående kategorier kan det innebära att ni behöver göra en konsekvensbedömning. Om två eller flera av punkterna är uppfyllda ska ni i de allra flesta fall göra en konsekvensbedömning. I tveksamma fall bör ni alltid göra en konsekvensbedömning. Ni bör överväga att göra en konsekvensbedömning om ni:

- *utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare*

- *behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande betydande följder för den registrerade*

- *systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer*

- *behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter*

- *behandlar personuppgifter i stor omfattning*

- *kombinerar personuppgifter från två eller flera behandlingar på ett sätt som den registrerade inte förväntar sig, till exempel när man samkör register*

- *behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, exempelvis barn, anställda, asylsökande, äldre och patienter*

- *använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)*

- *behandlar personuppgifter på ett sätt som hindrar de registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån."*

Dataskyddsombudet bedömer att flera kommuner och förvaltningar ännu inte har kommit i gång med sitt konsekvensbedömningsarbete tillräckligt och att den här delen därför bör vara ett av fokusområdena inför 2023. Dataskyddsombuden planerar att genomföra insatser med fokus på att stärka förmågan att komma i gång och genomföra konsekvensbedömningar i enlighet med definitionen i GDPR.

Rekommendationer från DSO:

- Fortsätt arbetet med att ta fram en strategi och rutin för konsekvensbedömningsarbetet.
- Kartlägg vilka ytterligare behandlingar ni har som kräver konsekvensbedömningar.
- Ta fram en tidsplan för arbetet och genomför konsekvensbedömningar för de behandlingar som kräver det.

Referenser

Artikel 29-arbetsgruppen (EDPB) Riktlinjer om öppenhet enligt förordning (EU) 2015/679 https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

Integritetskyddsmyndigheten (2022) h/ttps://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/fora-register-over-behandling/

Integritetsmyndigheten, (2022) https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/