Kultur- och utbildningsnämnden med dess förvaltning, Alingsås kommun

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:

Central dataskyddsorganisation
Kommunen har en central dataskyddsorganisation i kommunledningskontoret, den består bland annat av kommunjurist, informationssäkerhetsansvarig och IT-chef. Dessa funktioner stöttar övriga förvaltningar med dataskyddsarbete och driver nätverket för informationssäkerhet och dataskydd inom kommunen. I detta nätverk finns samtliga förvaltningar representerade och man jobbar i nätverket utefter en gemensam handlingsplan för informationssäkerhet och dataskydd så att samtliga förvaltningar har samma fokusområden under året. Bakom ovannämnda nätverk och funktioner finns fler roller och grupperingar som jobbar med informationssäkerhet och dataskydd centralt i kommunen. Den centrala dataskyddsorganisationen redogör själva mer för deras arbete och hur de är organiserade i sitt eget svar till DSO.

Dataskyddsorganisation inom kultur och utbildnings-förvaltningen
Ytterst ansvarig för dataskyddsarbetet är kultur och utbildningsnämnden. Inom kultur och utbildningsförvaltningen finns följande funktioner med i den interna dataskyddsorganisationen: förvaltningsjurist, systemutvecklare och administrativ chef. Dessa funktioner jobbar tillsammans i enlighet med den centrala dataskyddsorganisationens handlingsplan. Man arbetar även utefter den egna förvaltningens specifika behov gällande dataskyddsarbete. Frågor som rör dataskydd inom förvaltningens verksamheter lyfts och löses i förstahand av förvaltningens egna dataskyddsorganisation som vid behov ber om stöttning från den centrala dataskyddsorganisationen.

Ansvarsfördelning mellan central dataskyddsorganisation och förvaltningens dataskyddsorganisation

Den centrala dataskyddsorganisationens ansvar består av att identifiera, planera och samordna dataskyddsarbete som är relevant för samtliga förvaltningar. I deras arbete ingår även att bevaka nationella och internationella frågor som rör dataskydd och hålla sig uppdaterade. Samt stötta förvaltningarna generellt i arbete och frågor som rör dataskydd.

Förvaltningens dataskyddorganisations ansvar består av att arbeta i samklang med den centrala dataskyddsorganisationen och arbeta med de fokusområden som den centrala organisationen har sin plan. Inom förvaltningens ansvar ligger även att inventera, identifiera, planera och genomföra dataskyddsarbete kring områden som rör den egna förvaltningen. I detta ingår att se över vad i dataskyddsarbetet som behöver förbättras, vad som behöver följas upp och vad som behöver genomföras. Det kan röra sig om att ta fram rutiner som saknas för dataskydd, göra stickprov av efterlevnad av GDPR, uppdatera befintliga rutiner utefter nya lagar samt att föra ut dataskyddsarbete i verksamheterna och jobba för ökad medvetenhet kring frågorna. Åtgärder för att införliva dataskyddsarbete ute i förvaltningens verksamheter kan bestå av utbildningar, information och uppföljning av efterlevnad av befintliga rutiner. Både den centrala organisationen och förvaltningens organisation har i vissa frågor kontakt och söker vägledning från regionens dataskyddsombud.

Kultur och utbildnings-förvaltningens dataskyddsarbete

Kultur och utbildningsförvaltningens dataskyddsorganisation arbetar både enligt en egen handlingsplan inom förvaltningen som beskriver vilka fokusområden man kommer arbeta efter under året och den centrala handlingsplanen för informationssäkerhet och dataskydd. Förvaltningens egen handlingsplan är en kombination av de fokusområden som lyfts från central dataskyddsorganisation och utifrån förvaltningens verksamheters identifierade behov. Identifierade behov kan vara projektbaserade korta insatser eller längre pågående förbättringsarbeten. Tex. uppdatering av registerförteckning eller översyn av förvaltningens sociala medie-konton. Behov som identifieras under året fångas upp och läggs med i planeringen antingen under året eller för kommande år beroende på hur stor insatsen är samt hur brådskande arbetet anses vara. I dagsläget upplevs dataskyddsorganisationen fungera bra, både den centrala stöttande organisationen och den förvaltningsegna organisationen som de senaste åren lagt mer och mer fokus kring dataskyddsarbete. En av de förbättringsåtgärder som gjorts är att utöka förvaltningens dataskyddsorganisation genom att förstärka med rollen systemutvecklare som är ny sedan ett år tillbaka för att kunna satsa mer på dataskyddsfrågor framöver och jobba mer effektivt med dataskyddsfrågor inom förvaltningen. Det upplevs idag som att man har resurser med rätt kompetenser på plats för att styra arbetet och genomföra nödvändigt dataskyddsarbete och inom den egna förvaltningen. Det finns idag tillräckliga resurser för att genomföra nödvändigt dataskyddsarbete, men i takt med att omvärlden förändras, lagar och förordningar skärps och krav på dataskydd ökar i takt med mer utbredd digitalisering kan det komma att behövas både mer resurser och mer tid av befintliga resurser för att arbeta med dataskyddsfrågor på ett tillfredställande sätt.

Kultur och utbildningsförvaltningen verkar kontinuerligt för att öka medvetenheten kring vikten av dataskyddsarbete, varje anställds ansvar i att följa rutiner och riktlinjer som finns och komma med konkreta råd för hur det kan anpassas i varje

verksamhet. Förvaltningen jobbar på flera olika sätt för att öka medvetenheten i verksamheterna. Ibland tas information upp på verksamheternas APT. Information läggs regelbundet ut på kommunens intranät såsom påminnelse om att gallringsrutiner, policys för personuppgiftshantering, information om säkra digitala tjänster, hantering av personuppgiftsincidenter mm. Vid lärarnas uppstartsdag i augusti 2022 var temat säkerhet, framförallt skolsäkerhet men även informationssäkerhet och GDPR. Dessutom görs punktinsatser i verksamheter där man ser ett behov av det eller som av någon anledning blivit eftersatta.
Dokument

Bilaga 1: Handlingsplan informationssäkerhet och dataskydd 2022.
Bilaga 2. Handlingsplan dataskydd kultur och utbildningsförvaltningen.
Bilaga 3. Informationssäkerhetspolicy i Alingsås kommun.
Styrdokument i kommunen som beskriver hur en dataskyddsorganisation ska se ut utifrån informationssäkerhet. Det här dokumentet beskriver till viss del uppdelning av roller och ansvar inom kommunen gällande arbete med dataskydd.

Kommentar från DSO:

Dataskyddsombudet ser det som positivt att förvaltningen har en struktur där det övergripande dataskyddsarbetet bedrivs av den lokala dataskyddsorganisationen som består av funktionerna förvaltningsjurist, systemutvecklare och administrativ chef. Funktionerna arbetar tillsammans enligt den centrala dataskyddsorganisationens handlingsplan samt efter den lokala handlingsplanen och det egna förvaltningens specifika behov. Dataskyddsfrågor inom verksamheterna lyfts och löses i första hand av förvaltningens egen dataskyddsorganisation som vid behov ber om stöttning från den centrala organisationen. Med hänsyn till förvaltningens storlek och uppdrag utgör detta arbetssätt en bra grund och förstärker den organisatoriska modell som behövs i förhållande till kommunledningen och i förlängningen dataskyddsombuden. Det ger också förvaltningen goda förutsättningar att ta sig an dataskyddsarbetet och bedriva ett ändamålsenligt arbete där den lokala dataskyddsorganisationen får en samordnande roll som kan förmedla beslut och viktig information vidare till verksamheterna och samtidigt lyfta utmaningar och frågor till den centrala organisationen i kommunen.

Förvaltningen bör dock resonera vidare i hur den lokala dataskyddsorganisationen kan utvecklas och förtydligas. Dataskyddsarbetet ska inte ses som ett eget verksamhetsområde utan behöver integreras som ett naturligt inslag i förvaltningens samtliga processer. I detta arbete bör förvaltningen i ett första led utvärdera den lokala dataskyddsorganisationen och göra en bedömning av om den är ändamålsenlig och tillräcklig i förhållande till förvaltningens olika uppdrag och verksamheter. Arbetet bör dokumenteras och förankras.

Förvaltningen bör också resonera kring och överväga vilka resurser som är rimliga i förhållande till de olika verksamheternas personuppgiftsbehandlingar och risker knutna till dem. Det kan exempelvis handla om att definiera roller och

utse digitaliseringsombud ute i verksamheterna som kan sätta sig in i olika delar som behöver genomföras för att förvaltningen ska leva upp till dataskyddlagstiftningens 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:

Kultur- och utbildningsförvaltningen för ett behandlingsregister över samtliga av de verksamhetssystem/digitala tjänster som finns inom förvaltningen. Alla nya system som köps in skall in i registerförteckningen och registerförteckningen skall uppdateras kontinuerligt.

Under 2022 har man lagt extra fokus på att uppdatera registerförteckningen för utbildningsverksamhetens system och de allmänna system som hela förvaltningen nyttjar. Under resterande del av 2022 och under 2023 kommer man gå igenom och uppdatera resterande verksamheters delar i registerförteckningen. I denna uppdateringsprocess har även strukturen kring behandlingen ändrats något. Därav är registerförteckningen uppdelad i två olika dokument, en del som är uppdaterad och en del som behöver uppdateras och föras samman med det uppdaterade registret. I registerförteckningen finns information om vilken verksamhet som utför behandlingen, vilken nämnd som står som personuppgiftsansvarig, på vilken rättslig grund man lagrar uppgifterna, vilka typer av personuppgifter som behandlas, om det förekommer känsliga

personuppgifter, om uppgifter överförs till tredje land, information till den registrerade mm.

Vad gäller den generella utformningen av registerförteckningen så har kultur och utbildningsförvaltningen fått indikationer, bland annat från DSO vid deras besök i utbildningsverksamheten under våren 2022, på att man bör se över strukturen i kultur och utbildningsnämndens registerförteckning och göra om den och utgå utifrån behandling i stället för utifrån system. Kultur och utbildningsförvaltningen samverkar med nätverket för dataskydd och informationssäkerhet i kommunen och har lyft behovet av och vill samarbeta kring att ta fram en kommungemensam mall för registerförteckning och att man i det arbetet bör se över hur strukturen i behandlingsregistret är uppbyggd.

De vanligaste rättsliga grunderna för personuppgiftsbehandling som anges i registerförteckningen är:

- Fullgöra ett avtal i vilket den registrerade är part, art. 6.1 b. Exempelvis vid köp av webbiljett till badhus eller konserter.
- Utföra uppgift av allmänt intresse, art 6.1 e. Exempelvis när det kommer till att kunna tillhandahålla utbildningsverksamhet där elever behöver finnas registrerade för att tex. kunna få betyg eller genomföra prov. Ett annat exempel är biblioteksverksamhet för att kunna tillhandahålla bokutlåning.

Den rättsliga grunden samtycke används i mycket liten utsträckning inom kultur och utbildningsförvaltningen. Ett av de få tillfällena då det används är för personuppgiftsbehandling gällande olika former av bildanvändning, digitalt och tryckmaterial samt vid användandet av sociala medier framför allt när det kommer till gymnasieskolan. Bildanvändningen tillhör inte skolans grunduppdrag, men är ett verktyg för att visa och informera vad som händer i verksamheten, visa upp skolan för kommande elever och vårdnadshavare. Elev/vårdnadshavare anmäler samtycke till bildanvändning via e-tjänst. Anställda som hanterar sociala medier och bildanvändning kontrollerar alltid samtycke innan bildpublicering.

I dagsläget för kultur och utbildningsnämnden inget register för behandlingar där de är personuppgiftsbiträde. Det som kan sägas är att man endast har ett system där kultur och utbildningsnämnden står som personuppgiftsbiträde. Det rör utbildning i brandfarliga arbeten för plåt och svets-utbildningen. Här har man upprättat ett Personuppgiftsbiträdesavtal med den andra parten där det framgår att kultur och utbildningsnämnden i detta fall räknas som personuppgiftsbiträde. Men det ses som ett förbättringsområde inför framtiden att upprätta ett behandlingsregister som även fångar upp detta. Informations-skyldighet

Vad gäller informationsskyldighet till personal så får man information om hur personuppgifter behandlas när man skriver på sitt anställningsavtal och den finns även på kommunens intranät. Vad gäller informationsskyldighet till elever och vårdnadshavare så finns informationen länkad på skolplattformen Arena för

lärande och vid varje terminsstart går man ut med en nyhet om vart man hittar informationen.

För allmänheten finns information på Alingsås kommuns hemsida om hur personuppgifter behandlas när man skickar in ärenden/synpunkter till kommunen. Även i varje e-tjänst som finns för kommuninvånare och allmänheten informeras om hur personuppgifter behandlas.

I vissa fall kommer informationen in genom att den enskilde själv har lämnat informationen tex, vid köp av biljetter eller registrering för att kunna låna böcker på biblioteket. (art. 13 GDPR) I andra fall kommer informationen från andra system eller myndigheter. Tex. För elever som ska börja gymnasiet så kommer deras information in till kultur och utbildningsförvaltningen via Gr:s antagningssystem Indra och landar i kultur och utbildningsförvaltningens elevhanteringssystem (art. 14 GDPR).

I många fall går informationsflödet från kommunens metakatalog (centralt användar-register) till andra system inom förvaltningen. Tex. Så går personaldata från personalsystemet och elevdata från elevhanteringssystemet in till kommunens centrala metakatalog för att därifrån sedan gå vidare till andra system där personal och elever behöver kunna få en profil och logga in för att utföra arbete eller ta del av digitala tjänster för sin utbildnings skull.

Bilaga 4. Alströmers hantering av personuppgifter som ligger ute på arena för lärande.
Bilaga 5. Information till personal vid anställning
Bilaga 6. Utbildning och kommun-övergripande system
Bilaga 7. Resterande del av förvaltningens registerförteckning.

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 tittat närmare på de bifogade behandlingsregistren och kan se att förvaltningen blandat perspektiv. I huvudsak har man listat ett IT-system som en enskild behandling men ibland har man även listat en process och ibland en handlingstyp. Så länge man kan svara på de tidigare nämnda punkterna så ”går” det att upprätta ett register utifrån alla dessa perspektiv. Dock så är det 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.

Dataskyddsombudet har fått tillgång till ett behandlingsregister där förvaltningen agerar som personuppgiftsansvarig. Om förvaltningen också verkar som personuppgiftsbiträde är det viktigt att ni upprättar ett separat register även för dessa behandlingar.

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:

- Överväg att omarbeta registret så att det utgår från era processer/uppdrag och inte IT-system. Uppdragen återfinns främst i för verksamheten tillämplig lagstiftning men även beslut och avtal.
- Bedöm om ni har ett behov och skapa ett register för de behandlingar när förvaltningen agerar som personuppgiftsbiträde.
- 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:

Det finns en kommunövergripande rutin för hantering av personuppgiftsincidenter som Kultur och utbildningsförvaltningen använder sig av. I rutinen framgår ärendegången tydligt. Anställda som upptäcker/ får kännedom om en personuppgiftsincident behöver omedelbart kontakta sin närmaste chef. Chefen rapporterar in personuppgiftsincidenten i en intern e-tjänst som därifrån går direkt till förvaltningens GDPR-samordnare, in i förvaltningens diarium och till dataskyddsombudet. När GDPR-samordnaren får ärendet bedömer denne om incidenten skall anmälas till IMY, om anmälan skall gå vidare till IMY ordnar GDPR-samordnaren detta inom 72 timmar från dess att incidenten upptäcktes. Samtliga personuppgiftsincidenter och eventuella anmälningar till IMY diarieförs i förvaltningens diarium och återfinns i en samlad lista årsvis. Informationen om personuppgiftsincidenter och tillhörande rutin är åtkomlig för alla anställda på kommunens intranät, kommunportalen. Kultur och utbildningsförvaltningen informerar även regelbundet om vikten av att rapportera in personuppgiftincidenter och försöker öka kännedomen om rutinen genom nyhetsinlägg på kommunportalen eller via Arbetsplatsträffar. Kultur och utbildningsförvaltningen följer IMY:s rekommendationer och upplever att man tillgodoser dessa genom befintlig rutin som finns på plats och genom proaktivt arbete för att kunna hantera personuppgiftsincidenter inom förvaltningen. Under 2022 har 6 personuppgiftsincidenter rapporterats in inom förvaltningen. Inga av personuppgiftsincidenterna under 2022 har bedömts allvarliga nog för att skickas till IMY.

Bilaga 8. Rutin för personuppgiftsincident:

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 anmärkningsvärt 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 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:

Kultur och utbildningsförvaltningen har en rutin som skall göra processen enkel både för de registrerade att anmäla om de önskar ett registerutdrag och för handläggare att hantera ärendet. På kommunens hemsida finns en e-tjänst som är kommunövergripande där man kan anmäla att man som registrerad önskar ett registerutdrag. Man anger i e-tjänsten vilka nämnder man vill få registerutdrag ifrån och om man vill få det postat till sig eller hämta upp i rådhusets reception. Via e-tjänsten skickas en begäran till de valda nämnderna. Varje nämnd som tar emot en förfrågan om registerutdrag behandlar begäran inom sin egen verksamhet. En begäran om registerutdrag skall handläggas och lämnas ut inom 30 dagar från att den kommer in. Registrator skickar begäran vidare till GDPR-samordnare, förvaltningschef, verksamhetschefer och administrativ chef. Verksamhetschefer och administrativ chef ansvarar för att respektive verksamhetssystem samt verksamhetens egna register kontrolleras och fyller i bifogad mall för registerutdrag om den registrerades personuppgifter förekommer i något av verksamhetssystemen. Svar och ifyllda mallar skickas till GDPR-samordnare som sammanställer registerutdraget och skickar det till den registrerade. För rättelse eller radering av personuppgifter finns en kommungemensam rutin som kultur och utbildningsförvaltningen tillämpar. Den registrerade anmäler sin begäran i en e-tjänst på kommunens hemsida, även i detta fall anger den registrerade vilken nämnd begäran gäller. Begäran går till GDPR-samordnare för berörd nämnd som gör en bedömning om det är möjligt/lämpligt att radera personuppgifterna det rör sig om utifrån de rättsliga grunder som finns tex. arkivlagen. Oavsett om begäran om radering/rättelse får avslag eller går igenom meddelas den registrerade. En begäran om rättelse eller radering av personuppgifter skall enligt befintlig rutin hanteras skyndsamt. När det kommer till tillbakadragande av samtycke så saknas det i dagsläget en nedskriven rutin för detta.

Under 2022 har kultur och utbildningsnämnden hittills fått in väldigt få ärenden som rör registrerades rättigheter. Begäran om registerutdrag: 1. Rättelse och radering av personuppgifter: 0.

Bilaga 9. Rutin för rättelse och radering av personuppgifter:
Bilaga 10. Rutin begäran om registerutdrag

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:

Alla nya IT-system/tjänster som införskaffas eller befintliga avtal som förlängs skall innan de upphandlas/tecknas passera via förvaltningens GDPR-samordnare och systemutvecklare som utreder hur personuppgiftshanteringen och informationssäkerheten ser ut i det tilltänkta systemet. Tex. vilka personuppgifter som kan komma att hanteras i systemet och om det kommer att förekomma tredjelandsöverföring eller innehålla känsliga personuppgifter. Om dessa roller ser risker görs först en riskanalys och som sedan kan leda fram till att en konsekvensbedömning behöver genomföras. När det kommer till redan befintliga system så genomförs regelbundet genomlysningar av GDPR-samordnare och systemutvecklare utifrån förvaltningens behandlingsregister och dokumenthanteringsplan där man ser över olika aspekter såsom tredjelandsöverföring, hantering av känsliga personuppgifter, gallringsintervall mm. I de fall man ser att personuppgifter hanteras på ett sätt som inte är i linje med GDPR eller policys inom kommunen genomför man i första skedet en riskanalys som sedan kan övergå till en konsekvensbedömning vid behov. När en riskanalys eller konsekvensbedömning genomförs blir det ofta tydligt vilka risker som omfattas eller problem som kan uppstå. I vissa fall upptäcks att riskerna kan avhjälpas med rent tekniska åtgärder såsom att be leverantören genomföra åtgärder som tex. att byta ut en underleverantör som bryter mot GDPR eller att verksamheten själv inför åtgärder som rent tekniskt säkrar upp personuppgiftshanteringen i ett system. I de fall man hittar tekniska lösningar försöker man genomföra dessa, i alla fall går det inte att hitta den typen av lösning och i vissa fall kan man komma till slutsatsen att systemet bör avvecklas och ersättas med ett annat inom ett visst tidsintervall. Det finns en kommunövergripande e-tjänst som kan användas för att dokumentera både

riskanalys och konsekvensbedömning. Om man går vidare till steget konsekvensbedömning så skall konsekvensbedömningen skickas till Dataskyddsombudet för ett utlåtande. Förvaltningen saknar idag en nedskriven rutin för genomförandet av konsekvensbedömning men arbetar tillsammans med kommunens centrala dataskyddsorganisation för att ta fram de rutiner som saknas. Det stöd man använder sig av idag är IMY:s generella rekommendationer: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/ Det finns en kolumn i kultur och utbildningsnämndens behandlingsregister för konsekvensbedömningar för att man skall kunna bevaka och följa upp genomförda konsekvensbedömningar. Senaste konsekvensbedömningen som Kultur och utbildningsförvaltningen genomförde och skickade till DSO var för systemet Studybee ett system som hanterar omdömen för elever på gymnasiet och vuxenutbildningen. I detta fall hade man upptäckt att en av Studybees underleverantörer låg utanför EU/EES och att det då alltså handlade om tredje lands-överföring av personuppgifter. Denna konsekvensbedömning skickades till dataskyddsombudet som gav ett utlåtande. Under tiden som man på förvaltningen tog ställning till DSO:s utlåtande och började planera för åtgärder meddelande leverantören att de sagt upp sin amerikanska underleverantör och i stället bytt ut den mot en svensk underleverantör efter påtryckningar från flera kunder. Systemet kunde i detta fall behållas eftersom den identifierade risken upphört.

Bilaga 1. konsekvensbedömning av Studybee.

Kommentar från DSO:

Dataskyddsombudet ser det som positivt att förvaltningen har genomfört en konsekvensbedömning på ett av de system där man identifierat att det förelåg hög risk för registrerade och att förvaltningen i övrigt försöker att utveckla arbetet vad gäller konsekvensbedömningar. Det är också bra att förvaltningen har haft en kontakt med dataskyddsombudet i samband med bedömningen. 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 hör 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/