Kommunstyrelsen och Överförmyndarnämnden med respektive förvaltningar, 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:

Överförmyndarnämnden i Alingsås kommun har sin förvaltning i överförmyndarsamverkan med Lerums kommun. Överförmyndarsamverkan befinner sig organisatoriskt under kommunledningskontoret i Alingsås kommun. I alla relevanta delar vad gäller årskontrollen omfattas överförmyndarsamverkan av kommunstyrelsens arbete med dataskydd. Enheten är i praktisk mening att jämställa med en mindre verksamhetsenhet på kommunledningskontoret. Det som sägs nedan om kommunstyrelsen och kommunledningskontoret omfattar därför även överförmyndarnämndens verksamhet.

Dataskyddsarbetet drivs tillsammans med arbetet med informationssäkerhet och IT-säkerhet. Som grund ligger kommunens styrdokument Informationssäkerhetspolicy och Policy för behandling av personuppgifter. Organisationen definieras sedan i Riktlinjer för informationssäkerhet.

Hur arbetet ska bedrivas under 2022 anges i Handlingsplan för informationssäkerhet och dataskydd i Alingsås kommun 2022. Här anges bland annat de aktiviteter som ska genomföras under året för olika delar i dataskyddsorganisationen.

Kommunen har ett koncernövergripande nätverk för informationssäkerhet och dataskydd som träffas en gång per kvartal. Varje personuppgiftsansvarig inom kommunen har mellan en och tre representanter i nätverket. Sammankallande är IT-säkerhetsansvarig, informationssäkerhetsansvarig och samordnare för dataskydd. På nätverksträffarna delas omvärldsbevakning, handlingsplanen verkställs genom aktiviteter och påminnelser om egna aktiviteter och något tema inom områdena lyfts upp för information och diskussion. Mellan nätverksträffarna skickas ett nyhetsbrev ut med aktuell information inom de tre områdena.

Under 2022 har det upprättats en dataskyddsorganisation för kommunstyrelsens förvaltning kommunledningskontoret. Kommunledningskontorets

dataskyddsorganisation trädde i kraft under våren 2022. Organisationen syftar till att göra dataskyddsarbetet mer robust och mindre sårbart, jämfört med att ha en ansvarig person.

De roller som bildar kommunledningskontorets dataskyddsorganisation är:

- samordnare av kommunens dataskyddsfrågor,
- informationssäkerhetsansvarig,
- digitaliseringsansvarig,
- samordnare för konsekvensbedömningar av dataskydd samt personuppgiftsbiträdesavtal,
- samordnare för behandlingsregister,
- samordnare för personuppgiftsincidenter samt
- kommunarkivarie.

Syftet är också att bredda kompetensen kring dataskyddsfrågor inom kommunledningskontoret, vilket i sin tur kommer övriga förvaltningar till del då dessa roller finns för stöd och rådgivning i respektive fråga. De tillsatta rollerna kommer framöver även ansvara för att relevanta styrdokument, instruktioner, e-tjänster, mallar och stödjande dokument för processer tas fram för respektive område. De kommer även att bidra till rådgivning kring arbetet med frågorna hos varje personuppgiftsansvarig och i övrigt medverka till att verkställa de aktiviteter som beslutas politiskt i handlingsplanen för dataskydd och informationssäkerhet. Med en större grupp personer som arbetar med frågorna ökar även tillgängligheten för stöd i uppkomna frågor till övriga kommunkoncernen.

Kommunledningskontorets dataskyddsorganisation har precis inrättats och är därför omogen. Utbildningsinsatser kommer framöver att utföras för att säkra respektive rolls kompetens. Här kommer de utbildningsfilmer som vi fått del av från dataskyddsombuden att användas som grund för att höja kompetensen.

Resurser bedöms finnas då flera av kontorets avdelningar bidrar med arbetstid för de personer som bemannar dataskyddsorganisationen, bl.a. säkerhetsenheten, IT-avdelningen, upphandlingsenheten och kansli- och juridikenheten. Framöver tillkommer eventuellt även ekonomiska resurser för att bekosta utbildning att krävas, den stora kostnaden utgörs dock av arbetstid för berörda personer.

I dagsläget finns inte något antaget styrdokument som definierar kommunledningskontorets dataskyddsorganisation, vilket upplevs som en brist. Detta planeras tas fram och föreslås beslutas under 2023.

Kommentar från DSO:

Alingsås kommun har kommit långt i sitt dataskyddsarbete och har en god grund och en bra idé för hur kommunen vill arbeta för att främja ett starkt, stabilt och säkert dataskyddsarbete. Att ha en central dataskyddsorganisation med flertalet funktioner som strategiskt servar och bistår övrig verksamhet är ett resurseffektivt sätt att leda och styra kommunens dataskyddsarbete för att leva upp till dataskyddslagstiftningens krav. Den centrala organisationen tar med fördel fram förvaltningsgemensamma styrdokument, strategier, mallar och e-

tjänster samt processer. På så vis kan respektive förvaltning förlita sig på grundläggande stöd och vägledning från den centrala organisationen. Utöver den centrala organisationen finns i varje förvaltning en utsedd kontaktperson som har ansvaret för samordningen av personuppgiftshanteringen inom förvaltningen. En sådan ordning är en bra förutsättning och är i linje med den organisationsstruktur som behövs för ett hållbart dataskyddsarbete, dels med hänsyn till dataskyddslagstiftningen, dels utifrån samverkansavtalet. Det finns även ett kommunövergripande nätverk för informationssäkerhet och dataskydd som ses en gång per kvartal där varje personuppgiftsansvarig har en till tre representanter. Ett sådant forum ger goda möjligheter att förmedla och utbyta information samt att hantera diverse dataskyddsfrågor där de lokala funktionerna kan bidra med verksamhetsspecifik kompetens och ges möjlighet att resonera kring de bedömningar som slutligt följer av personuppgiftsansvaret.

Utifrån en kommunal organisationsstruktur är det dock respektive nämnd som svarar för sina personuppgiftsbehandlingar i egenskap av personuppgiftsansvarig. För att respektive förvaltning ska kunna ta sig an dataskyddsarbetet i den enskilda nämndens ansvarsområde behövs en anpassad och tillräcklig dataskyddsorganisation i förhållande till bland annat mängden behandlingar och risker knutna till dessa. För att utveckla och förtydliga kommunens lokala dataskyddsorganisationer (inklusive kommunledningskontoret) kan därför nuvarande organisationsform behöva utvärderas för att säkerställa så att man har tillräckliga resurser på plats i förvaltningarna för att arbeta med dataskyddsfrågor i den omfattning som krävs. I dagsläget kan det vara oklart vilka förväntningar som finns inte minst på den lokala organisationen men även den centrala. Detta kan med fördel utredas och behov bedömas samt dokumenteras så att förväntningarna överensstämmer i exempelvis var olika frågor ska landa och vem som ska utföra arbetet. Underlaget kan sedan användas när de lokala organisationerna resurssätts.

I arbetet med att förtydliga och stärka organisationen och förvaltningen kan förvaltningen utvärdera nuvarande organisation för att säkerställa att man har tillräckliga resurser på plats. Ett sätt att reda ut och få klarhet är att 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 förvaltningen utvärderar och kartlägger det egna behovet. En första tanke när man börjar se över 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 med angränsande lagstiftning 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 en tillräckliga dataskyddsorganisationer 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 omfattning i frågor som rör dataskydd.

Alingsås kommun i stort, men också förvaltningarna 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 eller uppdatera roller och ansvar.
- Genomföra en kartläggning över sitt nuläge för att ringa in förvaltningens behov av organisation inom området och ta fram eller uppdatera 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:

Den stora majoriteten av kommunstyrelsens behandlingar bedöms finnas dokumenterade i respektive avdelnings behandlingsregister.

Ett arbete har nyligen initierats för att ta fram en ny form och struktur för kommunens behandlingsregister, som i dagsläget benämns registerförteckningar. Arbetet bedrivs tillsammans av samordnare för behandlingsregister, samordnare för dataskydd, IT-chef, informationssäkerhetsansvarig, digitaliseringsansvarig samt IT-arkitekt.

Förhoppningen är att tillsammans skapa en förteckning som innehåller flera delar i olika lager, där behandlingsregistret utgör en del. Syftet är att inte behöva uppdatera flera olika dokument när någon behandling ändras, ett systemstöd byts ut eller liknande. Arbetet bedöms pågå minst under hela 2023. När en ny struktur har tagits fram kommer denna att föreslås för övriga personuppgiftsansvariga att applicera på sina behandlingsregister.

I handlingsplan har uppdraget givits till samtliga förvaltningar att uppdatera sina registerförteckningar under 2022, kvartal 2 och 3 och detta har påmints om vid nätverkets träffar under året. Samordnare för dataskydd har funnits tillgänglig för rådgivning. I handlingsplanen uttrycks aktiviteten enligt följande:

”Registerförteckningarna togs ursprungligen fram 2018 i samband med ikraftträdandet av dataskyddsförordningen. Med anledning av rättsutvecklingen på området behöver respektive personuppgiftsansvarig revidera sin registerförteckning, med ledning och stöd från den centrala dataskyddsorganisationen. Korrekta, systematiska och uppdaterade registerförteckningar ligger sedan till grund för det fortsatta dataskyddsarbetet.”

Gällande informationsskyldigheten har ingen aktivitet utförts under 2022. Informationen som ges till de registrerade vid insamling av personuppgifter har inte uppdaterats under året, åtminstone inte vad som är känt centralt på kommunledningskontoret. Information finns sedan tidigare på kommunens hemsida, och den har inte heller reviderats under året.

Länk till informationstext på alingsas.se: 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 tittat närmare på de bifogade behandlingsregistren och kan se att förvaltningen har blandat perspektiv. I huvudsak har man listat ett IT-system som en enskild behandling men ibland har man 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. Ett sådant exempel skulle kunna vara att ha en behandling som heter i stil med ”upphandling av varor och tjänster” Sedan i beskrivningen hänvisar man till upphandlingsreglerna som myndigheten lyder under och beskriver varför myndigheten har just det uppdraget och vad syftet/ändamålet är. Det måste framgå i beskrivningen så det går att förstå just ändamålet med uppdraget/behandlingen.

Valet av rättslig grund kopplat till en behandling är ännu 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 ”upphandling av varor och tjänster” likt exemplet ovan. Sedan kanske systemet är lämpligt för att hantera flera olika typer av ärenden och då kan man för varje enskilt uppdrag/ behandling i stället 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 blir det mer komplicerat att få en klar bild för vilka ärenden som systemet är till för och vilka olika uppdrag som ingår. 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 eller avtal. 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. I stället 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 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 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.

Dataskyddsombudet behöver utifrån skrivningen; *”Det ligger på dataskyddsombudet att kontrollera att det registret som förs av personuppgiftsansvarige visar på att behandlingarna utförs på rätt sätt.”,* i flertalet av de bifogade behandlingsregister, särskilt poängtera att det utifrån dataskyddsförordningens regelverk är personuppgiftsansvarig som har ansvaret för att föra register över sina personuppgiftsbehandlingar och att visa på att behandlingarna utförs i enlighet med dataskyddslagstiftningen.

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:

Alingsås kommun har en gemensam rutin för hantering av personuppgiftsincidenter. Rutinen omfattar vilka åtgärder som ska vidtas och vem som är ansvarig för respektive åtgärd vid en personuppgiftsincident.

Kommunledningskontorets samordnare för personuppgiftsincidenter har under våren och sommaren 2022 reviderat rutinen och uppdaterat den. I samband med detta togs även en mall för uppföljning fram för att underlätta just uppföljningen av en personuppgiftsincident.

För rapportering och stöd i hanteringen av en personuppgiftsincident finns en e-tjänst. E-tjänstens utformning säkerställer att alla väsentliga frågor gällande incidenten besvaras och hjälper ansvarig att kartlägga incidenten samt att vidta relevanta åtgärder.

Samordnare för hanteringen av personuppgiftsincidenter har informerat om den reviderade rutinen och e-tjänsten samt uppföljningsmall vid möte för nätverket för informationssäkerhet och dataskydd där samtliga nämnder, bolag och förbund finns representerade. Varje deltagare har sedan ett ansvar att föra informationen vidare till sina kollegor.

Det är svårt att bedöma om alla inträffade personuppgiftsincidenter dokumenteras. Kommunledningskontorets bedömning är dock att det finns en god kännedom inom kontoret gällande både skyldigheten att uppmärksamma och att dokumentera en personuppgiftsincident. Hur god kännedom som finns gällande vad som innebär en personuppgiftsincident kan dock säkerligen variera mellan anställda. Den allmänna medvetenheten om dataskydd bedöms dock så pass hög att den stora majoriteten anställda skulle fråga aktuella kollegor vid någon typ av händelse, och därigenom koppla in rätt kompetens för att göra bedömningen.

Kommunledningskontoret gör bedömningen att rutinen följer IMY:s rekommendationer för hantering av personuppgiftsincidenter. Vid framtagandet av rutinen för Alingsås kommun togs utgångspunkt i de riktlinjer som IMY (då Datainspektionen) presenterade på sin hemsida.

Personuppgiftsincidenter under 2022:

- Antal identifierade personuppgiftsincidenter hittills: en
- Antal personuppgiftsincidenter som anmäldes till IMY: noll

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. 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 bland annat genom att säkerställa att personuppgiftsincidenter hanteras enligt upprättad process i kommunens processverktyg. Att endast en incident uppmärksammats i verksamheten får dock anses anmärkningsvärt lågt och förvaltningen bör ställa sig frågan varför inte fler incidenter identifieras. Av den incident som hanterats visar dock förvaltningen förmåga i att hantera det inträffade men att man sedan valt att avstå att anmäla, 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. 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. Vid behov kan även dataskyddsombuden bistå med utbildningsinsatser inom området.

Rekommendationer från DSO:

- Analysera anledningen till att varför endast en incident identifierats och att denna inte ledde till en anmälan. Utred vilka insatser som kan stärka förmågan ytterligare inom förvaltningen, och genomför 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:

Verksamheten har goda förutsättningar att hantera de registrerades rättigheter i form av registerutdrag och begäran om rättelse eller radering av personuppgifter.

Bifogade rutiner för begäran om registerutdrag samt begäran om rättelse eller radering beskriver de processer som gäller för hantering av begäran om dessa.

Kommunledningskontoret bedömer att rutinen efterlevs och att de registrerade får vad de begärt inom utsatt tid.

Vi har inte någon rutin för att hantera ett tillbakadragande av samtycke. Än så länge har ingen sådan begäran inkommit till kommunstyrelsen. Utifrån avsaknaden av sådana begäranden hittills bedömer kommunledningskontoret att en sådan begäran kan hanteras av ansvariga personer utan fastställd rutin.

Antal begäranden gällande de registrerades rättigheter som hittills hanterats under 2022:

- Begäran om registerutdrag: fem
- Begäran om rättelse eller radering: noll
- Tillbakadragande av samtycke: noll

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. Man ska dock komma ihåg att informationsskyldigheten alltid blir gällande för varje behandling och är en passiv rättighet. Detta innebär att förvaltningen ska göra den registrerade uppmärksammad på att behandling av personuppgifter sker och varför. Det är som regel utifrån denna information som den registrerade har möjlighet att agera. Förvaltningen bör resonera kring de olika rättigheterna som följer av 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 verksamheten 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:

Det finns ingen framtagen rutin för hur arbetsprocessen för genomförandet av en konsekvensbedömning. Bedömningen görs i fall till fall och baseras endast på kunskap hos berörda personer.

Det de vid framtagandet hade till syfte att vara ett stöd i processen föra att bedöma om en konsekvensbedömning behövdes, samt hjälpa ansvarig att besvara rätt frågor. Utifrån ny kunskap i organisationen om konsekvensbedömningar och dess komplexitet behöver e-tjänsten revideras.

Kommentar från DSO:

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 istället 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 dels med anledning av svaret från kommunstyrelsens förvaltning, dels med anledning av att flera kommuner och förvaltningar ännu inte har kommit igång med sitt konsekvensbedömningsarbete tillräckligt att detta därför bör vara ett av fokusområdena inför 2023. Dataskyddsombuden planerar att genomföra insatser med fokus på att stärka förmågan att komma igång och genomföra konsekvensbedömningar i enlighet med definitionen i GDPR.

Rekommendationer från DSO:

- Ta fram en strategi och rutin för konsekvensbedömningsarbetet
- Kartlägg vilka 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/