Kommunövergripande tillämpningsanvisningar till Riktlinje för dataskydd

Dokumenttyp: Kommunövergripande tillämpningsanvisning

Antaget av: Kommundirektören 2024-03-22

Senast reviderat:

Giltighetstid: tills vidare

Diarienummer: KS 2024–323

Dokumentansvarig: Kommundirektör

Adresserat till: Samtliga förvaltningar

Tidpunkt för aktualitetsprövning:

Relaterade styrdokument: Riktlinje för dataskydd KS 2022–574

Sökord: Dataskydd, Dataskyddsombud, Dataskyddssamordnare, Konsekvensbedömning avseende dataskydd, Personuppgift, Personuppgiftsincident

1. Tillämpningsanvisningen

1.1. Inledning

Denna tillämpningsanvisning konkretiserar Linköpings kommuns dataskyddsarbete. Utöver denna tillämpningsanvisning kan och ska förvaltningsspecifika rutiner tas fram.

Kommunens dataskyddsarbete utgår från dataskyddsförordningen. Dataskyddsförordningen syftar till att skydda människors fri- och rättigheter, särskilt rätten till skydd för personuppgifter. Dataskyddsförordningen reglerar hur personuppgifter får behandlas. I Sverige finns även annan reglering inom området såsom den svenska dataskyddslagen med kompletterande bestämmelser som närmare reglerar hur personuppgifter får behandlas.

1.2. Syfte och omfattning

Syftet med denna tillämpningsanvisning är att tydliggöra hur kommunens dataskyddsarbete ska vara uppbyggt och bedrivas. I denna tillämpningsanvisning finns därför en beskrivning av kommunens övergripande dataskyddsarbete. Tillämpningsanvisningen gäller för alla kommunens nämnder och förvaltningar men riktar sig särskilt till förvaltningarnas dataskyddssamordnare och ledning.

1.3. Förhållningssätt

Kommunen ska aktivt arbeta med dataskydd. Förvaltningschefen har det övergripande ansvaret för att denna tillämpningsanvisning integreras i förvaltningens dagliga arbete bland annat genom att tillse att förvaltningen har relevanta rutiner och att dessa efterlevs.

1.4. Avgränsning

Tillämpningsanvisningen behandlar inte andra, till dataskydd, närliggande områden såsom informationssäkerhet, offentlighets- och sekretesslagens eller arkivlagens bestämmelser.

Informationssäkerhet och dataskydd syftar till att skydda information, vilket innebär att de i många fall samverkar. Enligt offentlighetsprincipen har allmänheten rätt att ta del av allmänna handlingar. Dataskyddsförordningen påverkar inte denna rätt, däremot kan dataskyddsförordningen påverka hur allmänna handlingar innehållandes personuppgifter får lämnas ut. Om det finns anledning att tro att eventuella personuppgifter som begärs ut kommer att behandlas i strid med dataskyddslagstiftningen råder det sekretess för uppgifterna enligt offentlighets- och sekretesslagen. Dataskyddsförordningen hindrar inte att kommunen och kommunala bolag bevarar och arkiverar allmänna handlingar. Gränsdragningen till dessa områden kommer inte att belysas närmare i denna tillämpningsanvisning.

1.5. Grundläggande principer

All personuppgiftsbehandling inom kommunen ska genomsyras av de grundläggande principerna för dataskydd:

Laglighet, korrekthet och öppenhet
Personuppgiftsbehandlingen ska stödjas på en rättslig grund och följa dataskyddsförordningen samt övrig tillämplig lagstiftning.

Behandlingen av personuppgifter ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade för att anses korrekt.
Öppenhet innebär att det ska vara tydligt för de registrerade hur deras personuppgifter behandlas och vilka rättigheter de har. De registrerade ska därför få information om detta på ett enkelt och begripligt sätt.

Ändamålsbegränsning
Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet får inte vara för brett eller otydligt angivet.
Om redan insamlade personuppgifter ska behandlas på ett nytt sätt, måste den nya behandlingen vara förenlig med det eller de ursprungliga ändamålen.

Uppgiftsminimering
Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. De uppgifter som behandlas ska vara tydligt kopplade till ändamålet. Det är alltså inte tillåtet att samla in uppgifter för obestämda framtida behov, för att de kan vara "bra att ha".

Riktighet
Personuppgifter som behandlas ska vara riktiga och uppdaterade. Uppmärksammas felaktiga uppgifter ska dessa, om möjligt, rättas.

Lagringsminimering
Personuppgifter ska sparas så länge de behövs för behandlingens ändamål. När personuppgifterna inte längre behövs för behandlingen ska de avidentifieras eller tas bort. Uppgifterna ska sparas efter att de slutat användas om det sker för arkivändamål av allmänt intresse eller på grund av andra lagkrav. Linköpings kommun utgör ett intensivdataområde, vilket innebär att handlingar rörande bland annat socialtjänst, vård- och individomsorg enligt lag ska bevaras hos Stadsarkivet i större utsträckning än i övriga delar av landet.

Integritet och konfidentialitet
Personuppgifter ska skyddas genom att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas.

Ansvarsskyldighet
Personuppgiftsansvarig ansvarar för att följa de grundläggande principerna om personuppgiftsbehandling. Principen om ansvarsskyldighet innebär även att den personuppgiftsansvarige ska kunna visa att, och på vilket sätt, principerna följs.

1.6. Rättsliga grunder

All personuppgiftsbehandling ska stödjas på en av de rättsliga grunderna för att vara laglig. Nedan följer de rättsliga grunder som bör ligga till grund för den personuppgiftsbehandling som kommunen utför. *Intresseavvägning* och *grundläggande intressen* är ytterligare rättsliga grunder men dessa bör inte vara tillämpliga för kommunens personuppgiftsbehandling.

Samtycke

Används endast i undantagsfall. Samtycket ska vara frivilligt och det får inte finnas en maktobalans mellan parterna. Den registrerade ska informeras om personuppgiftsbehandlingen och samtycket ska samlas in skriftligt. Den registrerade har rätt att när som helst återkalla sitt samtycke varpå personuppgiftsbehandlingen måste upphöra.

Avtal

När personuppgiftsbehandlingen är nödvändig, antingen för att fullgöra ett avtal med den registrerade eller för att vidta åtgärder innan avtalet ingås. Anställningsavtal är ett exempel.

Rättslig förpliktelse

När det framgår av lag att personuppgiftsbehandlingen måste ske.

Allmänt intresse eller led i myndighetsutövning

Allmänt intresse är den rättsliga grunden för övrig personuppgiftsbehandling som sker när kommunen behandlar personuppgifter inom ramen för sitt uppdrag och verksamhet.

När personuppgifter samlas in för att det ska fattas ett myndighetsbeslut till exempel gällande färdtjänst eller bistånd är den rättsliga grunden myndighetsutövning.

2. Dataskyddsorganisationen

2.1. Inledning

En tydlig och förankrad dataskyddsorganisation underlättar för kunskaps- och informationsspridning och tydliggör vilka arbetsuppgifter och vilket ansvar respektive medarbetare i organisationen har i dataskyddsarbetet.

Nämnderna ansvarar för att dataskyddsorganisationen ska kunna fullgöra sina uppgifter och för att skapa och upprätthålla en dataskyddskultur bland alla medarbetare. En förutsättning för att nämnderna ska kunna fatta adekvata beslut gällande dataskydd är att det finns en implementerad dataskyddsorganisation och rutiner som säkerställer att nämnden får lämplig kunskap och information.

Nedan följer en beskrivning av dataskyddsorganisationens olika delar och hur de samverkar inom kommunen.

2.2. Dataskyddsorganisationens uppbyggnad

Respektive nämnd inom kommunen är personuppgiftsansvarig för behandling som utförs inom dess ansvarsområde. Nämnd och förvaltning har således ansvar för kommunens dataskyddsarbete och är en del av kommunens dataskyddsorganisation. Inom dataskyddsorganisationen finns dessutom specifika roller vilka är kommunens dataskyddsombud och dataskyddssamordnare.

2.2.1. Förvaltningen

Det är förvaltningen som ansvarar för att utföra de uppgifter som följer av personuppgiftsansvaret och förvaltningen har därmed en nyckelroll i kommunens dataskyddsarbete.
Förvaltningschefen ansvarar för att dataskyddsarbetet är tydligt förankrat inom respektive förvaltning och för att en god dataskyddskultur etableras genom att frågorna prioriteras och följs upp inom förvaltningen. Det är förvaltningschefen, eller den som förvaltningschefen utser, som ska säkerställa att dataskyddsombudet i god tid rådfrågas i frågor som rör skydd av personuppgifter. Dataskyddsombuden ska tillhandahållas de resurser, den information och det stöd som krävs för att de ska kunna fullgöra sina uppgifter.

Det ska finnas en kontaktväg för dataskyddsombuden till förvaltningschefen, eller den som förvaltningschefen utser, dit information och/eller återkoppling som föranleder åtgärder från förvaltningens sida kan lämnas. Om dataskyddsombudens rekommendationer inte följs ska förvaltningschefen, eller den som förvaltningschefen utser, tillse att anledningarna till det dokumenteras.

Förvaltningschef ansvarar för att utse en eller flera dataskyddssamordnare så att förvaltningen alltid har minst en dataskyddssamordnare. Förvaltningschef ska säkerställa att dataskyddssamordnaren har tid, kompetens och lämplig funktion för att delta i dataskyddsorganisationens arbete. När en ny dataskyddssamordnare utses ska detta meddelas dataskyddsombuden i god tid. Den nya dataskyddssamordnaren ska ges tillgång till kommunens registerförteckning samt de kommunikationsvägar som delas av kommunens dataskyddsnätverk. Förvaltningen ska även se till att dataskyddsombuden vet vem på förvaltningen som hanterar incidenter vid dataskyddssamordnarens frånvaro.

2.2.2. Dataskyddsombud

Kommunstyrelsen ska utse dataskyddsombud för de kommunala nämnderna och erbjuda dataskyddsombud till bolagen i Stadshus AB-koncernen. Dataskyddsombudens arbete i de kommunala bolagen beskrivs inte närmare i denna tillämpningsanvisning. Dataskyddsombudens namn och kontaktuppgifter ska anmälas till tillsynsmyndigheten och det görs av dataskyddsombuden.

Rollen som dataskyddsombud är lagstadgad och arbetet bedrivs främst utifrån de uppgifter som framgår av dataskyddsförordningen. Dataskyddsombuden granskar efterlevnaden av dataskyddsförordningen och angränsande lagstiftning, rapporterar till ledningen genom att rapportera till förvaltningschefen, eller den som förvaltningschefen utser, samt vid behov till nämnd/styrelse och utgör kontaktpunkt för tillsynsmyndigheten och de registrerade. Dataskyddsombuden ska vidare informera och ge råd om dataskyddsförordningen inom kommunen samt utföra utbildnings- och informationsinsatser inom dataskyddsområdet. På grund av sin granskande och rådgivande roll är dataskyddsombuden inte operativa i kommunens dataskyddsarbete. Dataskyddsombuden har inte något eget ansvar för att kommunen följer dataskyddsförordningen utan ansvarar för att rapportera eventuella brister till ledningen.

Dataskyddsombuden rapporterar till ledningen bland annat genom att årligen ta fram en rapport med en aktuell lägesbild över förvaltningarnas dataskyddsarbete och förslag på förbättrande åtgärder. Dataskyddsombuden rapporterar även löpande till förvaltningen om brister som dataskyddsombuden upptäckt eller misstänker i den kontinuerliga dialogen med förvaltningens dataskyddssamordnare.

Därutöver utförs bland annat granskningar av nämndernas efterlevnad av dataskyddsförordningen och angränsande lagstiftning inom olika områden. Områdena för granskningarna som dataskyddsombuden utför väljer dataskyddsombuden utifrån sitt riskbaserade arbetssätt och granskningarna genomförs av dataskyddsombuden. Förvaltningarna ska medverka till att granskningarna kan genomföras på så sätt som dataskyddsombuden anvisar.

2.2.3. Dataskyddssamordnare

På varje förvaltning inom kommunen finns minst en dataskyddssamordnare som är ett stöd till sitt eller sina PM3-objekt och verksamheter i grundläggande frågor om dataskydd. Dataskyddssamordnaren ska arbeta utifrån förvaltningschefens styrning avseende vilka

verksamhetsrisker och åtgärder som ska prioriteras. Dataskyddssamordnaren förutsätts därför ha god kännedom om såväl verksamheten i stort som dess dataskyddsarbete. Som stöd till förvaltningschefen ska dataskyddssamordnaren leda, samordna och följa upp det operativa arbetet inom den egna förvaltningen. Det innebär att dataskyddssamordnaren bland annat bistår vid registreringar av personuppgiftsbehandlingar i kommunens registerförteckning och vid hantering av misstänkta personuppgiftsincidenter. Vid utvecklingen av bland annat rutiner och arbetssätt ska dataskyddssamordnaren involveras för att säkerställa att dataskyddslagstiftningen uppmärksammas. Dataskyddssamordnaren ska aktivt hålla sig uppdaterad om förvaltningens utvecklingsbehov inom dataskydd och vid behov meddela ansvarig chef.

Dataskyddssamordnaren fungerar som en länk mellan pm3-objektet, förvaltningen och dataskyddsombudet och ska ha kontinuerlig dialog med dataskyddsombudet bland annat i syfte att samråda med dataskyddsombudet och bistå vid granskningar av dataskyddsarbetet inom pm3-objekt eller förvaltning. Dataskyddssamordnaren ska löpande informera förvaltningen om det pågående dataskyddsarbetet. Dataskyddssamordnaren ska delta i kommunens dataskyddsnätverk.

2.2.4. Medarbetare

Alla medarbetare har ett ansvar för att behandlingen av personuppgifter utförs på ett korrekt sätt. Det är respektive chef som ansvarar för att riktlinjer, rutiner och arbetsinstruktioner är kända inom verksamheten.

2.2.5. Kommunjurist med informationssäkerhetsansvar

Inom kommunen finns en kommunjurist med informationssäkerhetsansvar som därmed även har kompetens inom dataskydd. Denne, eller dennes kollegor, kan bistå kommunens förvaltningar i frågor gällande dataskydd där dataskyddsombuden inte kan eller bör ge råd. Kommunjuristen har ingen granskande roll och kan därför vara ett kompletterande stöd i det operativa arbetet med dataskyddet. Som ovan beskrivits finns en nära koppling mellan informationssäkerhet och dataskydd. I de fall det behövs och inte är olämpligt sker därför en nära samverkan mellan den informationssäkerhetsansvariga kommunjuristen och dataskyddsombuden samt i viss mån även med dataskyddssamordnarna.

2.2.6. Dataskyddsnätverket

Till dataskyddsorganisationen hör ett dataskyddsnätverk bestående av kommunens dataskyddsombud samt dataskyddsamordnare från respektive förvaltning. Nätverket har till uppgift att stötta nämnderna och förvaltningarna i arbetet kring behandling av personuppgifter samt för utbyte av kunskaper och erfarenheter. Nätverket utgör även en möjlighet att planera och genomföra gemensamma insatser i verksamheterna, exempelvis utbildning inom dataskydd.

3. De registrerades rättigheter

3.1. Inledning

För att stärka rätten till skydd för personuppgifter har de registrerade ett antal rättigheter, i förhållande till kommunen, enligt dataskyddsförordningen. Detta avsnitt konkretiserar kommunens hantering av begäran om rättigheterna.

Det finns inga formkrav för hur en begäran om rättigheterna ska se ut. När en begäran inkommer till kommunen ska den hanteras snabbt, senast inom en månad, tidsfristen kan i vissa fall förlängas. Det är förvaltningen som ansvarar för att tillse att begäran hanteras korrekt. Kommunen ska alltid hantera begäran om rättigheter som inkommer men det innebär inte att alla begäranden kan tillmötesgås.

De vanligast begärda rättigheterna inom kommunen är rätten till information, rätten till tillgång (registerutdrag) och rätten till radering. Dessa rättigheter kommer att beskrivas närmare nedan. De registrerade har dessutom rätt att begära att:

- personuppgifter rättas
- begränsa en personuppgiftsbehandling,
- invända mot en behandlingen,
- utöva rättigheter vid automatiserade beslut och
- få dataportabilitet.

3.2. Kommunövergripande arbetssätt

Om en begäran om rättelse, begränsning, invändning, automatiserat beslutsfattande och dataportabilitet inkommer bör dataskyddsombuden rådfrågas för vidare hantering.

För hantering av begäran om rättigheter behöver den registrerades identitet säkerställas. Ett utlämnande av personuppgifter till fel individ kan orsaka en personuppgiftsincident. Nedan redogörs för de rättigheter som förekommer oftast i kommunens dataskyddsarbete.

3.2.1. Rätt till information

Information om personuppgiftsbehandlingen ska lämnas till de registrerade vid insamlandet av personuppgifter, till exempel vid nyanställning, på blanketter och vid e-tjänster. Informationen ska även lämnas vid andra tillfällen då den registrerade begär det.

Den information som ska lämnas till den registrerade är bestämd i dataskyddsförordningen och syftar till att ge den registrerade kontroll över hur dennes personuppgifter behandlas. Informationen ska till exempel omfatta vilken nämnd som är personuppgiftsansvarig, varför personuppgifterna behandlas och att den registrerade har rättigheter enligt dataskyddsförordningen. Informationen ska lämnas på ett lättbegripligt sätt, anpassat efter de registrerade. Kommunen lämnar ofta information i flera steg för att motverka informationsutmattning. Kommunen har en malltext för den information som ska lämnas i ett första steg.

3.2.2. Rätt till tillgång (registerutdrag)

En enskild har rätt att få veta om personuppgifter om den enskilda, eller barn som denne är vårdnadshavare för, behandlas och i så fall få tillgång till personuppgifterna i ett *registerutdrag*.

Skilj mellan begäran om registerutdrag enligt dataskyddsförordningen och en begäran om allmän handling enligt offentlighetsprincipen. För mer information om skillnaderna och om allmän handling, se Ärendehandboken.

Registerutdrag begärs via en e-tjänst på kommunens hemsida eller via Kontakt Linköping. Begäran ska handläggas av den personuppgiftsansvariga nämndens förvaltning. En begäran om registerutdrag ska som huvudregel skickas till den registrerades folkbokföringsadress.

Det är förvaltningen som tillser att de medarbetare som tar fram uppgifter till registerutdrag har rätt behörigheter för att kunna besvara begäran på ett korrekt sätt och resurser att undersöka förekomsten av personuppgifter i alla personuppgiftsbehandlingar. Observera att vissa uppgifter kan omfattas av sekretess även gentemot den enskilde själv eller gentemot ett barns vårdnadshavare. I de fall en enskild som har skyddade personuppgifter begär registerutdrag ska samråd ske med både dataskyddsombud och kommunjurist.

För att säkerställa att all nödvändig information meddelas den enskilde, ska den kommunövergripande rutinen med tillhörande mall för registerutdrag användas, se *”Registerutdrag avseende personuppgiftshantering”.* Den kommunövergripande rutinen hindrar inte att det vid behov tas fram kompletterande förvaltningsspecifika rutiner i samråd med dataskyddsombuden.

3.2.3. Rätt till radering

Registrerade har rätt att begära att få personuppgifter som behandlas om den registrerade raderade. Det finns undantag till rätten till radering, exempelvis kan allmänna handlingar inte raderas utan gallringsbeslut. Detta innebär att en begäran om radering inte alltid kommer kunna tillmötesgås. Oavsett om begäran kommer kunna tillmötesgås har den registrerade rätt att få ett överklagbart beslut. Av respektive delegationsordning framgår vem som har mandat att fatta ett sådant beslut.

Dataskyddsombuden ska alltid kontaktas omgående när en begäran om radering inkommit till kommunen.

4. Hantering av personuppgiftsincidenter

4.1. Inledning

Detta avsnitt konkretiserar kommunens hantering av misstänkta personuppgiftsincidenter. Kommunen ska aktivt arbeta för att personuppgiftsincidenter inte ska inträffa. Om en misstänkt personuppgiftsincident upptäcks ska förvaltningarna prioritera hanteringen av den misstänkta personuppgiftsincidenten, dels för att minimera konsekvenserna för de registrerade som drabbats, dels för att vidta åtgärder som motverkar att liknande incidenter uppstår.

Det är viktigt att förvaltningens medarbetare har kunskap om hur en misstänkt personuppgiftsincident ska hanteras. Notera att en och samma incident kan behöva rapporteras till olika stödfunktioner såsom dataskyddsombuden, LKDATA eller tjänsteman i beredskap.

För att säkerställa en korrekt hantering av misstänkta personuppgiftsincidenter behöver förvaltningsspecifika rutiner för hanteringen tas fram utifrån detta avsnitt. Den förvaltningsspecifika rutinen hindrar inte att det vid behov tas fram enhetsspecifika/verksamhetsspecifika rutiner. Rutinerna ska tas fram i samråd med dataskyddsombuden.

4.2. Vad är en personuppgiftsincident?

En personuppgiftsincident är en händelse som leder till att personuppgifter som behandlas förloras, ändras, förstörs eller avslöjas för obehöriga. En incident kan uppstå på grund av misstag, tekniska fel eller med avsikt. Exempel på händelser som kan utgöra personuppgiftsincidenter är:

- Systemfel eller skadlig programvara som förstör personuppgifter
- Stöld av datorer, telefoner eller andra enheter
- Dokument med personuppgifter skrivs ut på fel skrivare
- Dokument med personuppgifter försvinner
- En anställd lånar ut personligt användarnamn och lösenord
- Ett mail med personuppgifter skickas till fel mottagare
- En person har felaktig behörighet i ett system och får på så vis felaktig tillgång till personuppgifter
- Personuppgifter är inte tillgängliga för de som behöver dem och det leder till negativa konsekvenser för de registrerade.

En personuppgiftsincident kan leda till skador eller risk för skador för de registrerade. Exempel på sådana skador är:

- förlust av kontrollen över de egna personuppgifterna,
- begränsning av rättigheter,
- identitetsstöld eller bedrägeri,
- ekonomisk förlust,
- obehörigt hävande av pseudonymisering,
- skadat anseende,
- förlust av konfidentialitet, eller
- annan ekonomisk eller social nackdel för den berörda fysiska personen.

Misstänkta personuppgiftsincidenter som upptäcks ska åtgärdas, utredas, dokumenteras och vid behov anmälas till tillsynsmyndigheten IMY.

Incidenter ska anmälas till IMY om det inte är osannolikt att incidenten leder till risk för de registrerades fri- och rättigheter. En sådan anmälan ska ske inom 72 timmar från det att incidenten upptäckts. Det är därför viktigt att alla misstänkta incidenter utreds i den utsträckning som krävs för att förvaltningen, i samråd med dataskyddsombudet, ska kunna avgöra om incidenten ska anmälas till tillsynsmyndigheten, inom 72 timmar. I vissa fall finns det möjlighet att komplettera en påbörjad anmälan efter att 72 timmar har passerat.

4.3. Kommunövergripande arbetssätt

Inom kommunen ska alla misstänkta personuppgiftsincidenter rapporteras till dataskyddsombuden via dataskyddsombudens sida på Linweb. Dataskyddsombuden rapporterar sedan incidenten vidare till ansvarig förvaltnings dataskyddssamordnare för vidare hantering.

Förvaltningen ansvarar för att misstänkta incidenter utreds inom rätt tid. Detta innebär att förvaltningen ska driva arbetet med utredningen skyndsamt genom att bland annat ansvara för att ta fram den information som behövs, kalla till möten samt vid behov kontakta stödfunktioner. Det är därefter den, eller de, på förvaltningen särskilt utsedde medarbetaren som efter samråd med dataskyddsombuden beslutar om incidenten är sådan att den ska anmälas till tillsynsmyndigheten eller endast dokumenteras hos nämnden.

Förvaltningen ansvarar för att anmälan och eventuell komplettering görs till tillsynsmyndigheten i rätt tid och att anmälan respektive de allmänna handlingarna kring incidenten diarieförs.

I vissa fall, när incidenten leder till hög risk för registrerades fri- och rättigheter, ska även de drabbade informeras om incidenten. Det är den, eller de, på förvaltningen särskilt utsedde medarbetaren som, efter samråd med dataskyddsombuden, beslutar om de drabbade ska informeras och på vilket sätt detta ska ske.

Det är viktigt att ha i åtanke att en incident som först bedöms vara en it-säkerhetsincident eller en informationssäkerhetsincident också kan vara att betrakta som en personuppgiftsincident, och vice versa.

5. Upprätthållande av registerförteckning

5.1. Inledning

Dataskyddsförordningen ställer krav på ett strukturerat dataskyddsarbete. Den personuppgiftsansvarige ska, som följd av detta, bland annat föra ett register över de personuppgiftsbehandlingar som utförs av och åt den personuppgiftsansvarige. Ett sådant register kallas registerförteckning och det ska innehålla viss, i förordningen bestämd, information om respektive personuppgiftsbehandling. Registerförteckningen är även ett viktigt verktyg för den personuppgiftsansvarige i dataskyddsarbetet eftersom den ger en lättillgänglig överblick över de personuppgiftsbehandlingar som utförs.

5.2. Kommunens registerförteckning

Samtliga personuppgiftsbehandlingar som utförs inom nämndernas respektive ansvarsområden ska registreras i en registerförteckning. Inför en ny behandling eller om en behandling förändras eller avslutas ska registerförteckningen uppdateras. Respektive nämnds registerförteckning finns samlad i ett kommungemensamt system. Alla nämnder inom kommunen ska hantera sina respektive registerförteckningar på samma övergripande sätt, därför kommer samtliga registerförteckningar inom kommunen beskrivas gemensamt som *registerförteckningen*.

Registerförteckningen består av formulär där information om personuppgiftsbehandlingen registreras. Den information som ska registreras utgår från kraven i dataskyddsförordningen.

5.3. Kommunens arbetssätt

Det är förvaltningen som tillser att registerförteckningen uppdateras, så att den information som vid var tid finns i registerförteckningen är aktuell och korrekt. Det är därför viktigt att arbetet med registerförteckningen beaktas i olika processer som påverkar förvaltningens personuppgiftsbehandlingar till exempel vid införande eller avveckling av nytt it-system eller en ny rutin.
Det är dataskyddssamordnaren som själv eller genom annan registrerar informationen som lämnas. Dataskyddssamordnaren ska aktivt arbeta för att registerförteckningen är uppdaterad och komplett.

Dataskyddsombuden granskar registerförteckningen löpande för att säkerställa att den information som ska finnas enligt dataskyddsförordningen finns angiven för respektive registrering. Registerförteckningen kan därutöver utgöra underlag för dataskyddsombudens planering, rådgivning och granskning avseende såväl själva registerförteckningen som övrigt dataskyddsarbete.

6. Konsekvensbedömning avseende dataskydd

6.1. Inledning

När en ny personuppgiftsbehandling planeras, som kan leda till hög risk för de registrerade, ska en konsekvensbedömning avseende dataskydd genomföras. Konsekvensbedömningen ska följa en personuppgiftsbehandling, därmed kan konsekvensbedömningen komma att följa personuppgifterna genom fler än ett system.

Konsekvensbedömning avseende dataskydd är en process för att utreda vilka risker som finns med en specifik personuppgiftsbehandling och ta fram åtgärder för att minska dessa risker. Genom att i ett tidigt skede ta ställning till frågor som hur många uppgifter som ska samlas in, vilken rättslig grund som är tillämplig och för vilka ändamål uppgifterna får behandlas, minskar risken för att en redan påbörjad behandling senare måste förändras för att hänsyn inte har tagits till dataskyddsförordningens krav.

Konsekvensbedömningen utgör även ett verktyg för att visa att de grundläggande principerna enligt dataskyddsförordningen efterlevs, vilket är en skyldighet som åligger den personuppgiftsansvarige enligt principen om ansvarsskyldighet. Konsekvensbedömningen är en pågående process som behöver omprövas och uppdateras kontinuerligt.

Den personuppgiftsansvariges skyldighet att utreda och vidta lämpliga riskminimerande åtgärder, och i övrigt efterleva dataskyddsförordningen, påverkas inte av om en konsekvensbedömning behöver genomföras eller inte.

Det är förvaltningen som tillser att konsekvensbedömningar genomförs och uppdateras, så att konsekvensbedömningen vid var tid är aktuell och korrekt. Det är därför viktigt att arbetet med konsekvensbedömningen beaktas i olika processer som påverkar förvaltningens personuppgiftsbehandlingar.

I de fall konsekvensbedömningen avseende dataskydd kan ske i samband med exempelvis genomförande av riskanalys avseende NIS, ska dessa samplaneras och genomföras parallellt. Representant från förvaltningen bör i dessa fall vara en person som har kännedom om såväl personuppgiftsbehandling som kontinuitetshantering.

6.2. Kommunövergripande arbetssätt

Konsekvensbedömningen ska genomföras i rätt tid av medarbetare som har god insikt i personuppgiftsbehandlingen. Arbetet med konsekvensbedömningen bör påbörjas så fort det är praktiskt möjligt och i takt med att personuppgiftsbehandlingens olika delar fastställs ska konsekvensbedömningen uppdateras. Om flera liknande personuppgiftsbehandlingar planeras kan dessa bedömas inom ramen för samma konsekvensbedömning.

Den kommungemensamma mallen för konsekvensbedömning avseende dataskydd ska användas. Dataskyddsombuden ska hållas uppdaterad och löpande rådfrågas vid

genomförandet av en konsekvensbedömning. Dataskyddsombuden ger råd och besvarar frågor om konsekvensbedömningen men på grund av sin granskande roll kan de inte vara operativa. Vid behov kan istället dataskyddssamordnaren vara ett stöd i arbetet.

När konsekvensbedömningen är färdigställd ska den diarieföras tillsammans med övriga handlingar i ärendet såsom huvudavtal och personuppgiftsbiträdesavtal. Konsekvensbedömningen ska ses över regelbundet och uppdateras vid behov.

6.2.1. Förhandsbedömning

Det första avsnittet i konsekvensbedömningen kallas *förhandsbedömning*. Förhandsbedömningen gör det möjligt att bedöma om personuppgiftsbehandlingen innebär en sådan hög risk för de registrerade att en fullständig konsekvensbedömning behöver genomföras.

När förhandsbedömningen är genomförd ska samråd ske med dataskyddsombuden för rådgivning kring vidare hantering. Dataskyddsombuden lämnar rekommendationer kring bedömning av risken. Om förvaltningen bedömer att risken är hög måste en fullständig konsekvensbedömning genomföras. I tveksamma fall bör en fullständig konsekvensbedömning göras. Om förvaltningen, trots dataskyddsombudets rekommendationer att fortsätta arbetet, anser att risken inte är så hög att en fullständig konsekvensbedömning ska genomföras, ska beslutet att inte gå vidare motiveras och dokumenteras i förhandsbedömningen.

6.2.2. Fullständig konsekvensbedömning avseende dataskydd

För de fall att en fullständig konsekvensbedömning ska genomföras fortsätter arbetet enligt anvisad mall. I konsekvensbedömningen beskrivs personuppgiftsbehandlingen från början till slut med särskilt beaktande av behandlingens nödvändighet och proportionalitet. I en väl genomförd konsekvensbedömning besvaras hur alla de grundläggande principerna kommer tillgodoses.