Kungsbacka

Hantering av personuppgifter

Riktlinjer

Dokumentegenskaper:	Titel: Hantering av personuppgifter
Beslutad av:	Kommunfullmäktige 5 mars 2024 § 33, KS-2023-00815
Gäller från:	2024-03-05
Ansvarig förvaltning:	Kommunstyrelsens förvaltning
Kontakt:	Kungsbacka direkt 0300-83 40 00 | info@kungsbacka.se Kungsbacka kommun, 434 81 Kungsbacka www.kungsbacka.se

Innehåll

Kungsbacka kommuns riktlinjer för hantering av personuppgifter är ett komplement till kommunens integritetspolicy. Riktlinjerna gäller för kommunens nämnder, inklusive kommunstyrelsen och revisionen.

Inledning

De här riktlinjerna tydliggör hur GDPR:s krav förverkligas i Kungsbacka kommun. Syftet är att säkerställa att kommunen hanterar personuppgifter korrekt och likvärdigt, och att visa för allmänhet och anställda att de kan känna sig trygga med att deras personuppgifter hanteras på ett respektfullt sätt.

Samtidigt som kommunens nämnder är självständiga personuppgiftsansvariga är de också del av Ett Kungsbacka. För att kunna utföra kommunens uppdrag är det nödvändigt att lösa vissa uppgifter gemensamt och ha vissa gemensamma digitala system.

Riktlinjerna tydliggör nämndernas ansvar för olika uppgifter enligt GDPR samt deras skyldigheter gentemot varandra och de registrerade. Riktlinjerna klargör ansvar och gränser när kommunens nämnder är personuppgiftsbiträden åt varandra eller har gemensamt personuppgiftsansvar. Dokumentet innehåller också instruktioner för behandlingen som gäller när en nämnd utför personuppgiftsbehandling för en annan nämnds räkning, som personuppgiftsbiträde.[1]

[1] Styrdokumentet binder nämnderna gentemot varandra och tjänar som såväl rättsakt enligt artikel 28.3 som ”arrangemang” artikel 26.1 GDPR

Förhållandet mellan riktlinjerna och kommunens systemförvaltarmodell

Kungsbacka kommun arbetar enligt en kommungemensam modell för digitala tjänster och system. Modellen kallas *Modellen för digitala tjänster och system* och den beskriver bland annat hur förvaltning och utveckling av system ska bedrivas. Enligt modellen finns det utsedda roller för varje digital tjänst och system som kommunen använder. Rollerna utses vid anskaffningen.

Inom ramen för systemförvaltarmodellen framgår ansvaret för system och tjänster med avseende på säkerhet, funktionalitet och budget. Inom rollernas ansvar ligger också ansvar för att följa upp att de tekniska och organisatoriska krav som ställs på systemleverantören i egenskap av personuppgiftsbiträde följs. Ägaren har det yttersta ansvaret för en digital tjänst eller system. Budgetansvarig ansvarar för att godkänna årlig förvaltningsplan och uppföljningsrapport.

När det i de här riktlinjerna anges att den nämnd som har ägarskapet ansvarar för en viss uppgift, avses den nämnd där den utsedda ägaren är anställd. I regel ska det vara samma nämnd som har rätt att besluta om personuppgiftsbiträdesavtal enligt riktlinjerna nedan.

Det är alltid personuppgiftsansvarig som är ansvarig för den behandling som sker i systemet.

Kommunens bolag och stiftelse

Eksta bostads AB, med dotterbolag, och stiftelsen Tjolöholm är fristående juridiska personer som inte omfattas av de här riktlinjerna. Vid likartade behov kan upphandling av kommungemensamma system omfatta även dem. Behandlingen måste då regleras genom separata personuppgiftsbiträdesavtal för bolaget och stiftelsen.

Bolaget och stiftelsen kan använda det kommungemensamma dataskyddsombudet som dataskyddsombud för sin verksamhet.

Bolaget och stiftelsens dataskyddskontakter kan också delta i kommunens nätverk för dataskyddskontakter, gemensamma utbildningar och erfarenhetsutbyten.

Organisation

Varje nämnd är personuppgiftsansvarig

Varje nämnd är personuppgiftsansvarig för den personuppgiftsbehandling som sker i den egna verksamheten. Varje nämnd ska därför säkerställa att det finns tekniska och organisatoriska förutsättningar för att uppfylla de krav som ställs på personuppgiftsansvariga enligt dataskyddslagstiftningen.[2] Personuppgiftsansvaret kan inte delegeras.

Personuppgiftsansvaret är omfattande och följande lista ger vägledning för vad som ingår. Listan är inte uttömmande.

Personuppgiftsansvarig ansvarar enligt dataskyddslagstiftningen bland annat för att:

- Följa upp att personuppgiftsbehandlingen följer gällande dataskyddslagstiftning,
- försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
- upprätthålla behandlingsregister över samtliga personuppgiftsbehandlingar i den ansvariges verksamhet,
- säkerställa att medarbetarna har nödvändig kompetens för att kunna följa dataskyddslagstiftningen,
- säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning,
- säkerställa att personuppgiftsincidenter hanteras i enlighet med lagstiftningens krav,
- utse dataskyddsombud och anmäla dess kontaktuppgifter till tillsynsmyndigheten. Stödja dataskyddsombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens.

Kommunstyrelsen

Leder och samordnar

Kommunstyrelsens förvaltning ska leda, styra och samordna kommunens arbete med att uppfylla kraven i dataskyddslagstiftningen. Det inbegriper bland annat att ta fram och samordna övergripande information, rutiner och dokumentmallar. Kommunstyrelsens förvaltning sammankallar kommunens nätverk för dataskyddskontakter och rekryterar eller upphandlar ett kommungemensamt dataskyddsombud.

[2]Med ”dataskyddslagstiftningen” avses EU:s allmänna dataskyddsförordning, GDPR (Europaparlamentet och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG) och kompletterande svensk lagstiftning på dataskyddsområdet: exempelvis dataskyddslagen, brottsdatalagen och tillämpliga registerförfattningar som patientdatalagen, lagen om behandling av personuppgifter inom socialtjänsten och tillhörande förordningar.

Ansvarar för kommunövergripande informationssystem

Av kommunstyrelsens reglemente framgår att kommunstyrelsen är ansvarig för kommunövergripande informationssystem. Med det avses digitala tjänster och system som används av alla nämnder. Kommunstyrelsen har processer och rutiner för att identifiera och ta hänsyn till de olika personuppgiftsansvariga nämndernas behov vid anskaffning av kommungemensamma digitala tjänster och system. Den mest skyddsvärda informationen ska sätta standarden för lämpliga skyddsåtgärder. Genom att anskaffa system gemensamt kan högre kvalitet, samordningsvinster och bättre möjligheter att ställa krav uppnås.

Kommunstyrelsens ansvar för kommungemensamma system omfattar att systemets funktionalitet och säkerhet motsvarar de krav som behöver ställas utifrån den avsedda behandlingen, och att leverantören uppfyller de krav som ska ställas på personuppgiftsbiträden enligt dataskyddslagstiftningen och de här riktlinjerna. Respektive personuppgiftsansvarig nämnd ansvarar för att den egna behandlingen i de kommunövergripande systemen har laglig grund och följer de grundläggande principerna om personuppgiftsbehandling och att systemet inte används för annan behandling än vad som avsetts.

Biträdande kommundirektör fattar beslut om att teckna personuppgiftsbiträdesavtal för kommungemensamma system genom delegation från samtliga andra nämnder.

Kommungemensamma stödprocesser

Kommunstyrelsen har i uppgift enligt sitt reglemente att utföra vissa kommungemensamma stödprocesser, som inbegriper behandling av personuppgifter. När behandlingen omfattar personuppgifter som rör andra nämnders anställda, brukare, kunder eller leverantörer etc. är kommunstyrelsen gemensamt personuppgiftsansvarig med respektive annan nämnd. Se mer nedan under rubriken *kommungemensamma stödprocesser* i nästa avsnitt.

Nämnden för Service

Nämnden för Service ansvarar för service till kommunens invånare, till anställda och till övriga förvaltningar i kommunen. Nämnden för Service har också en viktig roll för kommunens dataskydd genom att den ansvarar för kommunens IT-infrastruktur och kommunintern drift, utveckling och support av system.

Nämnden utför många kommungemensamma stödprocesser för de andra nämndernas räkning. I många fall förutsätter det behandling av en stor mängd av kommunens personuppgifter. När behandlingen omfattar personuppgifter som rör andra nämnders anställda, brukare, kunder, leverantörer etc. är nämnden för Service gemensamt personuppgiftsansvarig med respektive annan nämnd. Se mer nedan under rubriken *kommungemensamma stödprocesser* i nästa avsnitt.

Nämnden för Service får fatta beslut om att teckna personuppgiftsbiträdesavtal för den behandling som behövs för att utföra sina uppgifter enligt reglemente, vilket inbegriper rätt att besluta om vilka biträden som ska anlitas för IT-infrastruktur.

När nämnden för Service ansvarar för drift, utveckling, teknisk säkerhet, underhåll och support av system som driftas internt, är nämnden för Service personuppgifts-biträde till de nämnder som använder systemet. Se mer nedan under rubriken *interna personuppgiftsbiträden*.

Dataskyddsombudet

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen ska agera självständigt och får inte ta emot instruktioner eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter. Dataskyddsombudet rapporterar till högsta ledningen såsom nämnd eller styrelse.

Dataskyddsombudet har bland annat i uppdrag att övervaka efterlevnaden av dataskyddslagstiftningen och att informera och ge råd för att efterleva lagen. Kommunens dataskyddsombud är placerat centralt på kommunstyrelsens förvaltning men arbetar på uppdrag av respektive nämnd, bolag och stiftelse som har utsett kommunens dataskyddsombud som dataskyddsombud för sin verksamhet.

Dataskyddskontakterna

Dataskyddskontakten är en stödfunktion för personuppgiftsansvarig nämnd, förvaltningens ledning och verksamhet. Ansvaret för att lagstiftning efterlevs vilar alltid på personuppgiftsansvarig och ansvaret kan inte delegeras. Dataskyddskontakten har bland annat följande uppgifter:

- Uppdatera och följa upp behandlingsregistren.
- Samordna och besvara registrerades begäran om att utöva sina rättigheter som exempelvis begäran om registerutdrag, radering och invändning.
- Följa upp att nödvändiga rutiner och instruktioner finns tillgängliga och är kända inom den egna verksamheten.
- Vara stöd vid upprättande av personuppgiftsbiträdesavtal, konsekvensbedömning avseende dataskydd och utredning av personuppgiftsincidenter.
- Vara stöd vid bedömning av om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten (IMY) och om de registrerade ska informeras om incidenten.
- Vara förvaltningens eller bolagets representant i det kommunövergripande nätverket för dataskyddskontakter.
- Samordna förvaltningens arbete med uppföljning och egenkontroll av dataskyddet.
- Samarbeta med dataskyddsombudet och fungera som länk mellan dataskyddsombudet och personuppgiftsansvarig
- Omvärldsbevaka kring personuppgiftsfrågor generellt och utifrån det egna verksamhetsområdet.
- Rådfråga och samråda med dataskyddsombudet för verksamhetens räkning, bland annat i samband med konsekvensbedömning avseende dataskydd.

Personuppgiftsbiträden och gemensamt personuppgiftsansvar inom kommunen

Kommunens myndigheter är självständiga personuppgiftsansvariga, samtidigt som de tillhör samma organisation och är underordnade kommunfullmäktiges beslutanderätt.

För att utföra kommunens uppdrag effektivt och likvärdigt är det nödvändigt att vissa saker görs gemensamt för alla nämnders verksamheter. Det är också nödvändigt att två eller flera nämnder kan samarbeta för att utföra kommunens uppdrag. Det innebär att personuppgifter ibland måste delas mellan olika personuppgiftsansvariga inom kommunen.

Nedan följer en beskrivning av fördelning av ansvaret för personuppgifts-behandlingen och skyldigheterna enligt GDPR vid gemensamt personuppgiftansvar mellan två eller flera nämnder och när en nämnd är personuppgiftsbiträde åt en eller flera andra nämnder.

Gemensamt personuppgiftsansvar

Inom kommunens verksamhet behöver samma personuppgifter ibland behandlas av olika personuppgiftsansvariga nämnder som har sina egna ändamål och sina egna lagliga grunder för behandlingen. När två eller flera personuppgiftsansvariga gemensamt beslutar om ändamål och medel för behandlingen kallas det för gemensamt personuppgiftsansvar.

Det kan exempelvis vara att nämnder med närliggande verksamhetsområden handlägger ärenden rörande samma personer i ett verksamhetssystem som de delar, eller att vissa kommungemensamma stödprocesser utförs av kommunstyrelsens förvaltning eller av förvaltningen för Service.

Samarbete mellan två eller flera nämnder

När två eller flera nämnder samarbetar om personuppgiftsbehandlingen och är gemensamt personuppgiftsansvariga, ansvarar de var för sig för att behandlingen följer dataskyddslagstiftningen och kommunens riktlinjer.

Varje nämnd ansvarar för den del av behandlingen som ligger inom den egna verksamheten enligt reglementet och får utföra de behandlingsåtgärder som behövs för att genomföra sina respektive uppdrag. Ansvaret för behandlingen inbegriper att säkerställa att den egna behandlingen har laglig grund och uppfyller de krav som ställs enligt dataskyddslagstiftningen.

Den som ska ha ägarskapet över systemet kan ges fullmakt av de andra personuppgiftsansvariga nämnderna att underteckna personuppgiftsbiträdesavtal med utomstående leverantör.

De gemensamt personuppgiftsansvariga nämnderna ansvarar var för sig för att förteckna behandlingen i sitt behandlingsregister. I behandlingsregistret ska också antecknas vilken annan nämnd personuppgiftsansvaret är gemensamt med och om nämnden för Service ansvarar för drift av systemet.

Kommungemensamma stödprocesser

Kommunstyrelsen respektive nämnden för Service utför båda vissa kommungemensamma stödprocesser. Exempel på det är att nämnden för Service utför rekrytering, löneadministration och har kontaktcenter för alla nämnders räkning eller att kommunstyrelsen bevakar kommunens kundreskontra.

Kommunstyrelsen respektive nämnden för Service har då som ändamål att utföra sina uppgifter enligt reglemente, medan respektive annan nämnd har ett annat ändamål med behandlingen. Personuppgiftsanvaret är då gemensamt. Undantaget

är när nämnden för service sköter IT-drift, då nämnden för service istället är personuppgiftsbiträde. Se rubriken *interna personuppgiftsbiträden* nedan.

Varje nämnd ansvarar för den del av behandlingen som ligger inom den egna verksamheten enligt reglementet och får utföra de behandlingsåtgärder som är nödvändiga för att genomföra sina respektive uppdrag. Ansvaret för behandlingen inbegriper att säkerställa att den egna behandlingen har laglig grund och uppfyller de krav som ställs enligt dataskyddslagstiftningen och de här riktlinjerna.

Kommunstyrelsen respektive nämnden för Service beslutar om vilka digitala verktyg och system som ska anskaffas för att utföra kommungemensamma stödprocesser som de ansvarar för. De ansvarar inför de andra nämnderna för att de biträden som anlitas uppfyller de krav som ställs på personuppgiftsbiträden enligt GDPR, kompletterande lagstiftning och de här riktlinjerna.

Vilka kommungemensamma stödprocesser kommunstyrelsen respektive nämnden för Service ansvarar för framgår av deras respektive reglementen och informationshanteringsplaner.

Interna personuppgiftsbiträden

När en nämnd sköter drift, utveckling, tekniskt underhåll eller support av ett system som en annan nämnd använder för sin personuppgiftsbehandling är den nämnden personuppgiftsbiträde. I regel är det Nämnden för Service som är internt personuppgiftsbiträde för andra nämnder inom Kungsbacka kommun.

När en nämnd agerar personuppgiftsbiträde för en annan nämnd ska den uppfylla de krav som ställs på personuppgiftsbiträden enligt dataskyddslagstiftningen och de här riktlinjerna.

Publika tjänster och myndighetstjänster

Kommunen använder sig av publika tjänster och myndighetstjänster, vilket i vissa fall inbegriper personuppgiftsbehandling. Gemensamt för publika tjänster och myndighetstjänster är att Kungsbacka kommun inte kan ställa krav på funktionalitet och inte heller äger informationen i systemet.[3] Det ska därför inte tecknas något personuppgiftsbiträdesavtal gällande dessa tjänster.

Varje personuppgiftsansvarig inom kommunen bär själv ansvaret för att nyttja dessa tjänster på ett sätt som stämmer överens med dataskyddslagstiftningen. Som stöd kan kommunstyrelsens förvaltning besluta om kommungemensamma styrdokument för användningen av vissa tjänster.

Uppgifter enligt dataskyddslagstiftningen

Under följande rubriker fastställs de olika nämndernas ansvar för olika uppgifter enligt GDPR.

Behandlingsregister

Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över sina behandlingar av personuppgifter (behandlingsregister).

[3] För mer information om publika tjänster och myndighetstjänster se dokumentet *Modell för digitala tjänster och system*.

Behandlingsregister ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Integritetsskyddsmyndigheten, IMY. Vad som ska finnas med i registret beskrivs i artikel 30 i dataskyddsförordningen.

I Kungsbacka kommun används behandlingsregistren också som ett sätt att dokumentera i vilka fall det finns gemensamt personuppgiftsansvar mellan nämnder och om nämnden för Service – eller någon annan nämnd – är personuppgiftsbiträde för en viss behandling.

Personuppgiftsansvarig nämnd

Varje nämnd ska löpande föra ett register över vilka personuppgifter som behandlas i den egna verksamheten. Behandlingsregistret ska utgå ifrån en processorienterad klassificeringsstruktur. Utöver de uppgifter som anges i artikel 30 GDPR ska det anges vilket system som används samt laglig grund för behandlingen. Om systemet är kommungemensamt ska det anges. Om nämnden för Service – eller någon annan nämnd – är personuppgiftsbiträde för behandlingen ska det anges.

Gemensamt personuppgiftsansvar

Kommungemensamma stödprocesser

Kommunstyrelsen och nämnden för Service för register över behandlingen för de kommungemensamma stödprocesser som de utför. Utöver de uppgifter som anges i artikel 30 ska det också anges vilket system som används, att det är gemensamt personuppgiftsansvar med övriga nämnder och om nämnden för Service ansvarar för drift av systemet.

De andra nämnderna ska notera behandlingen och ange vilken nämnd av nämnden för Service eller kommunstyrelsen som ansvaret är gemensamt med.

Andra samarbeten

I andra fall då två eller flera nämnder samarbetar och har gemensamt personuppgiftsansvar ska varje nämnd förteckna behandlingen. I registret ska också anges vilket system som används och vilken eller vilka nämnder som personuppgiftsansvaret är gemensamt med.

Nämnd som är personuppgiftsbiträde

Nämnden för Service – eller en annan nämnd som är personuppgiftsbiträde – ska föra register över de behandlingar som den utför för andra nämnders räkning. I registret ska anges de uppgifter som framgår av artikel 30.2 GDPR.

I förteckningen ska det anges systemets namn och behandlingens föremål, vilka kategorier av behandling som nämnden utför och vilka nämnder som använder systemet. För behandlingens ändamål, behandlingens varaktighet, typ av personuppgifter och kategorier av registrerade hänvisas till respektive personuppgiftsansvarig nämnds behandlingsregister.

Incidentrapportering

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att fri- och rättigheterna inskränks. En

personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller på annat sätt kommit i orätta händer genom exempelvis obehörig åtkomst eller obehörigt röjande.

En personuppgiftsincident ska anmälas till IMY inom 72 timmar från att den personuppgiftsansvarige har fått vetskap om incidenten. Om det är osannolikt att incidenten medför risk för enskilda personers fri- och rättigheter behöver incidenten dock inte anmälas till IMY, se artikel 33 GDPR.

Alla incidenter ska rapporteras så fort de upptäcks genom en intern e-tjänst för incidentrapportering. Anmälan tas emot av dataskyddskontakt på den berörda förvaltningen.

Som huvudregel är det den personuppgiftsansvariga nämnden som utreder, dokumenterar och anmäler incidenten till tillsynsmyndigheten.

Om en personuppgiftsincident beror på ett fel eller intrång i ett kommungemensamt system gör istället kommunstyrelsen eller nämnden för Service, beroende på vem av dem som har ägarskap över systemet, detta. De personuppgiftsansvariga nämnder som berörs ska informeras om incidenten och om kommunstyrelsens respektive nämnden för Services utredning, bedömning och hantering. Dokumentation av incidenten skickas till de berörda nämnderna för kännedom.

Om en personuppgiftsincident beror på ett fel eller intrång i ett system som används gemensamt av två eller flera nämnder, men som inte är kommungemensamt, ska den nämnd som har ägarskap över systemet ansvara för utredning, dokumentation och anmälan.

Det är alltid den personuppgiftsansvariga som bär ansvaret för att en personuppgiftsincident som ska anmälas blir anmäld. Om en personuppgifts-ansvarig nämnd inte håller med ägarnämndens bedömning att anmälan inte behövs, ska den själv anmäla incidenten.

Dataskyddsombudet ska alltid underrättas om en inträffad personuppgiftsincident och ges möjlighet att följa ärendets handläggning.

Anmälda incidenter ska följas upp och analyseras av varje förvaltning inom ramen för det systematiska dataskyddsarbetet. Kommunstyrelsens förvaltning följer även upp på kommunövergripande nivå inom ramen för sin uppsiktsplikt.

Underrättelse till de registrerade

Om en incident sannolikt leder till en hög risk för enskilda personers fri- och rättigheter måste de registrerade underrättas utan onödigt dröjsmål. Ansvaret för att det sker ligger på personuppgiftsansvarig men berörda roller på flera förvaltningar behöver samarbeta för att säkerställa att information kan lämnas så snart som möjligt och på lämpligt sätt. Vägledande för vem som gör vad ska vara vad som är mest effektivt. Om incidenten beror på ett fel eller intrång i en tjänst eller system som används av flera nämnder samordnar den nämnd som har ägarskapet arbetet.

Konsekvensbedömning

Om en behandling sannolikt leder till en hög risk för fysiska personers fri- och rättigheter ska en konsekvensbedömning avseende dataskydd göras. Konsekvensbedömningen ska göras innan behandlingen påbörjas och dataskyddsombudet ska rådfrågas. Konsekvensbedömningen görs för att

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att sänka dessa risker
- visa att man uppfyller GDPR:s krav.

Tröskelanalys

För att avgöra om en behandling sannolikt leder till en hög risk ska en tröskelanalys göras. Tröskelanalysen ska dokumenteras. Analysen utgår från fastställda kriterier.[4] Om fler än två av kriterierna är uppfyllda ska en konsekvensbedömning som huvudregel genomföras. Konsekvensbedömning är obligatoriskt om behandlingen ”sannolikt leder till hög risk för fysiska personers rättigheter och friheter”.[5] Även om en behandling uppfyller två eller flera kriterier kan bedömningen vara att behandlingen sannolikt inte leder till hög risk. Då ska en motivering till bedömningen dokumenteras och dataskyddsombudet ska ges tillfälle att yttra sig.

Samarbete om konsekvensbedömning

Det är den personuppgiftsansvariga som är ansvarig för att se till att en konsekvensbedömning utförs, men den kan genomföras av någon annan.[6] En enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker.

En konsekvensbedömning kan även vara gemensam för flera personuppgiftsansvariga, exempelvis kommunala myndigheter, när liknande teknik används för att samla in samma slags uppgifter för samma slags ändamål. När en gemensam konsekvensbedömning görs för flera personuppgiftsansvariga kallas det för referenskonsekvensbedömning.[7]

I Kungsbacka kommun ska vi sträva efter att göra tröskelanalyser och konsekvensbedömningar gemensamt så långt det är möjligt. Kommunstyrelsen gör tröskelanalyser och referenskonsekvensbedömningar för kommungemensamma digitala tjänster och system. När det är lämpligt gör nämnden för Service referenskonsekvensbedömningar för de system och tjänster som nämnden ansvarar för inom ramen för sitt uppdrag enligt reglemente.

En referenskonsekvensbedömning gäller för alla personuppgiftsansvariga nämnder och delas med de andra nämnderna. En personuppgiftsansvarig som inte håller med om bedömningen i en gemensam tröskelanalys eller referenskonsekvensbedömning är oförhindrad att ta fram en separat konsekvensbedömning för sin behandling. Referenskonsekvensbedömningen kan också kompletteras utifrån det egna verksamhetsområdet.

En gemensam konsekvensbedömning kan också tas fram av två eller flera nämnder inom kommunen, eller i ett annat lämpligt samarbete – till exempel med nämnder i andra kommuner som planerar för en liknande behandling.

---

[4] Kriterierna finns i artikel 35.3 GDPR och i en förteckning som beslutats av Datainspektionen, numera IMY. Kriterierna är inarbetade i den mall för konsekvensbedömning som tagits fram av kommunstyrelsens förvaltning.
[5] Artikel 35.1, illustrerat av artikel 35.3 och kompletterat av artikel 35.4, GDPR
[6] Artikel 29-gruppens riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Sid 16
[7] Artikel 29-gruppens riktlinjer om konsekvensbedömning, Sid 8

En referenskonsekvensbedömning delas eller görs allmänt tillgänglig. Åtgärder som beskrivs i konsekvensbedömningen ska genomföras och det ska motiveras varför en enda konsekvensbedömning har utförts.

De registrerades rättigheter

De personer vars personuppgifter behandlas kallas för *de registrerade*. Enligt dataskyddsförordningen har de registrerade ett antal rättigheter gentemot personuppgiftsansvariga. Kungsbacka kommun har en gemensam e-tjänst för att använda rätten till tillgång (registerutdrag), rättelse, återkallelse av samtycke, begränsning, dataportabilitet, invändning mot behandling och radering.

E-tjänsten finns publicerad på kommunens hemsida och i anslutning till den ges information om de registrerades rättigheter. Tjänsten är gemensam för samtliga personuppgiftsansvariga nämnder inom kommunen, inklusive kommunstyrelsen och revisionen, och begäran handläggs enligt kommungemensamma processer för respektive rättighet. Kommunstyrelsens förvaltning tar emot de ärenden som kommer via e-tjänsten och samordnar handläggningen.

Registrerade som inte kan använda sig av e-tjänsten har möjlighet att få hjälp inom ramen för kommunens serviceskyldighet.

Flera av de registrerades rättigheter gäller i begränsad omfattning i offentlig förvaltning. En begäran från den registrerade ska prövas och den registrerade ska få ett beslut som kan överklagas om begäran avslås. Vilka beslut som kan överklagas framgår av 7 kap. 2 § dataskyddslagen.

En begäran som riktar sig mot flera personuppgiftsansvariga i kommunen handläggs gemensamt av kommunstyrelsens eller nämnden för Service förvaltning om det är lämpligt.[8] Beslut måste dock fattas av varje personuppgiftsansvarig för sig.

Information till de registrerade

Den registrerade har rätt att få information om personuppgiftsbehandlingen. Vad informationen ska omfatta regleras i dataskyddslagstiftningen.

Generell information om kommunens personuppgiftsbehandling publiceras på kommunens hemsida. Kommunstyrelsen ansvarar för den kommunövergripande informationen, medan varje personuppgiftsansvarig nämnd ansvarar för att lämna information om sin egen behandling.

Information ska i många fall också lämnas när personuppgifterna samlas in. Om, och hur, information ska lämnas måste avgöras från fall till fall. Varje personuppgiftsansvarig ansvarar för att informationsskyldigheten uppfylls i den egna verksamheten.

Riktlinjer för Personuppgiftbehandlingen

Externa biträden och underbiträden

Personuppgiftsansvariga inom Kungsbacka kommun anlitar endast personuppgiftsbiträden och underbiträden som ger tillräckliga garantier om att

[8] Det är inte lämpligt med gemensam handläggning om begäran rör känsliga personuppgifter eller sekretessbelagd information som inte är lämplig att dela utanför myndighetsgränsen.

genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddslagstiftningen och säkerställer att de registrerades rättigheter skyddas.

Personuppgiftsbiträdesavtal ska alltid tecknas. Personuppgiftsbiträdesavtal ska säkerställa att hanteringen sker i enlighet med kraven i artikel 28.3 a-h i GDPR och nedanstående riktlinjer.

Lämplig säkerhet för personuppgifterna

Informationen i kommunens digitala tjänster och system ska klassas utifrån Kungsbacka kommuns rutin för informationsklassning. De informations-säkerhetskrav som kommit fram genom informationsklassningen, och ytterligare krav som kommit fram genom eventuell konsekvensbedömning utgör de krav på lämplig säkerhet som ska ställas vid behandling av personuppgifterna. Dessa krav ska dokumenteras och följas upp inom ramen för *modellen för digitala tjänster och system*.

Kommunstyrelsen ansvarar för att informationsklassning genomförs avseende kommungemensamma digitala tjänster och system.

För övriga system tillhandahåller kommunstyrelsen specialistkompetens som stöttar vid informationsklassningen.

Överföring av personuppgifter till tredje land

Kungsbacka kommun ska sträva efter att personuppgifter hanteras och lagras inom EU/EES.

Om personuppgifter förs över till tredje land ska det ske i överensstämmelse med kapitel 5 i GDPR och en så kallad överföringsanalys[9] ska göras. Om det gäller känsliga personuppgifter ska en särskild analys göras av om överföringen överensstämmer med artikel 9.3.

Vid risk för överföring till tredje land på grund av att det tredje landet har en lagstiftning som gör att personuppgiftsbiträdet kan bli skyldig att dela uppgifter med myndigheterna i landet, ska skydds- och kontrollåtgärder vidtas så att ett tillräckligt skydd uppnås.

Överföring av personuppgifter mellan system

Personuppgifter i kommunens system får föras över via tekniska integrationer till och från system inom kommunen, under förutsättning att personuppgifterna behövs för ändamålet med behandlingen i det mottagande systemet och det inte är oförenligt med det ursprungliga ändamålet, enligt artikel 5.1 b GDPR.

Personuppgifter får inte föras över om det mottagande systemet inte har en lämplig säkerhet för uppgifterna.

Vidareutnyttjande av personuppgifter inom kommunen

Innan personuppgifter behandlas för ett annat ändamål än de samlats in för ska det göras en analys av om det nya ändamålet är förenligt med det ursprungliga. Vid bedömningen ska, enligt artikel 6.4 GDPR, hänsyn tas till

[9] Transfer Impact Assessment

- sambandet mellan det ursprungliga ändamålet och det nya ändamålet
- i vilket sammanhang uppgifterna samlades in (vilket är förhållandet mellan kommunen och den enskilda personen?)
- uppgifternas typ och karaktär (är de känsliga?)
- möjliga konsekvenser av den avsedda vidare behandlingen (hur kommer den att påverka den enskilda personen?)
- huruvida det har vidtagits lämpliga skyddsåtgärder (såsom kryptering eller pseudonymisering).

Om uppgifterna samlats in grundat på *samtycke* eller enligt ett *lagstadgat krav*, är ingen vidare behandling möjlig utanför de områden som omfattas av det ursprungliga samtycket eller lagkravet. Vidare behandling kräver i så fall ett nytt samtycke eller en ny rättslig grund och att uppgifterna istället samlas in på nytt.

Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål anses inte vara oförenlig med de ursprungliga ändamålen.

Sekretess

Inom kommunen gäller tystnadsplikt enligt offentlighets- och sekretesslagens (OSL) bestämmelser. Utöver det ska personuppgifter alltid behandlas varsamt och konfidentiellt. Behörighet till personuppgifter ska bara ges till anställda och osjälvständiga uppdragstagare[10] som behöver tillgång till uppgifterna för att utföra sina uppgifter. Det ska finnas rutiner för att regelbundet granska vilka som har tillgång till personuppgifter och ta bort behörigheter som inte längre behövs.

När ett externt personuppgiftsbiträde eller underbiträde anlitas ska det säkerställas att de personer som har tillgång till personuppgifter omfattas av lagstadgad eller avtalsrättslig tystnadsplikt. Avtalsrättslig tystnadsplikt är inte alltid tillräcklig. En bedömning måste göras utifrån den aktuella informationen.

Gallring och bevarande av personuppgifter

Vid gallring och arkivering av personuppgifter ska gällande lagstiftning och kommunens styrdokument gällande arkivering och informationsförvaltning tillämpas.

När ett externt personuppgiftsbiträde eller underbiträde anlitas ska det säkerställas att biträdet är skyldig att radera eller återlämna alla personuppgifter och radera eventuella kopior när personuppgiftsbehandlingen upphör.

Inspektion och granskning

Kommunens samlade personuppgiftsbehandling granskas genom ordinarie rutiner för intern kontroll och revision. Därutöver ska varje personuppgiftsansvarig nämnd och styrelse bedriva ett systematiskt egenkontrollarbete. Granskning görs även av kommunens dataskyddsombud. Samtliga nämnder ska kunna tillhandahålla den information som behövs för granskning av personuppgiftsbehandlingen.

[10] Här menas konsulter och andra uppdragstagare som står under myndighetens ledning på ett sådant sätt att den omfattas av OSL. Se 2 kap 1 § andra stycket OSL.

Kommunstyrelsen och nämnden för Service har ett utökat ansvar för att kunna redovisa att de digitala tjänster och system som används kommunövergripande uppfyller de krav som ställs och att personuppgiftsbehandlingen följs upp löpande.

Alla personuppgiftsbiträdesavtal som ingås med externa parter ska vara utformade så att biträden och underbiträden är skyldiga att tillhandahålla den information som behövs för att granska så att de krav som ställs uppfylls.

Inbyggt dataskydd och dataskydd som standard

För system där personuppgifter behandlas ska principerna om *dataskydd som standard* och *inbyggt dataskydd* beaktas. Dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Inbyggt dataskydd innebär att hänsyn ska tas till integritets- och dataskyddsprinciperna redan när IT-system och rutiner utformas.