Kungsbacka

Riktlinjer för hantering av personuppgifter

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

1. Syfte

Riktlinjernas syfte är att säkerställa att kommunen hanterar personuppgifter på ett korrekt och likvärdigt sätt, men också att visa för allmänhet och anställda att de kan känna sig trygga med att deras personuppgifter hanteras på respektfullt sätt.

2. Nämndernas och kommunstyrelsens ansvar

2.1 Personuppgiftsansvariga och personuppgiftsbiträden

Personuppgiftsansvar måste som minimum ligga på myndighetsnivå. Varje nämnd är därmed personuppgiftsansvarig för de personuppgifter som behandlas i nämndens verksamhet, vilket också framgår av det gemensamma reglementet för kommunstyrelsen och nämnderna. Varje nämnd ansvarar därmed för att de legala kraven som ställs på personuppgiftsansvariga enligt allmänna dataskyddsförordningen, GDPR,[1] samt kompletterande lagstiftning[2] och förordningar uppfylls. De nämnder vars verksamhet omfattar verkställande av straffrättsliga påföljder är även personuppgiftsansvariga enligt brottsdatalagen och brottsdataförordningen[3].

För det fall en nämnd behandlar personuppgifter för en annan nämnds räkning är den nämnden personuppgiftsbiträde i GDPR:s mening, och får enbart behandla personuppgifter i enlighet med den personuppgiftsansvariga nämndens instruktioner. I denna situation har nämnden även att följa de bestämmelser som gäller för personuppgiftsbiträden enligt dataskyddsförordningen, samt det som anges i *Regler för interna personuppgiftsbiträdesförhållanden i Kungsbacka kommun*. Se även nedan under rubriken *8.2.*

Kommungemensamma digitala tjänster och system samt förvaltningsspecifika digitala tjänster och system som används av flera förvaltningar har enligt *Modellen för digitala tjänster och system* en utsedd ägare. I de fall den digitala tjänsten eller systemet innefattar personuppgiftsbehandling för flera personuppgiftsansvariga nämnder agerar i många fall den nämnd som innehar ägarskapet över systemet eller tjänsten personuppgiftsbiträde för de övriga nämnderna.

2.2 Kommunstyrelsens ansvar

Kommunstyrelsens förvaltning ska leda, samordna och ha uppsikt över kommunens arbete med att uppfylla kraven i GDPR och de nationella dataskyddsbestämmelserna. Det inbegriper bland annat att ta fram och samordna övergripande information, rutiner och dokumentmallar.

2.3 Samordningsuppdrag

Kommunstyrelsen kan själv, eller ge en annan nämnd i uppdrag att, samordna personuppgiftsbehandling som är lika över nämndgränserna, exempelvis i publika tjänster eller myndighetstjänster.

För kommungemensamma digitala tjänster och system samt förvaltningsspecifika digitala tjänster och system som används av flera förvaltningar har den nämnd som utövar ägarskapet i regel uppdraget att samordna

[1] Europaparlamentets 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 (allmän dataskyddsförordning)

[2] Bl.a lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), patientdatalagen (2008:355), totalförsvarsdatalagen (2020:151), Lag (2001:454) om behandling av personuppgifter inom socialtjänsten och kap. 26a kap. i skollagen (2010:800)

[3] Brottsdatalag (2018:1177) och brottsdataförordning (2018:1202)

personuppgiftsbehandlingen. Samordningsuppdraget övertar inte personuppgiftsansvaret utan syftar till att underlätta administreringen och skapa likvärdighet i personuppgiftshanteringen mellan de personuppgiftsansvariga nämnderna i kommungemensamma processer.

Samordningsuppdraget innebär bland annat att registrera behandlingen i den samordnande nämndens registerförteckning, underhålla information och beskrivningar om behandlingen samt bistå med samordning vid hantering av personuppgiftsincidenter och registrerades åberopande av sina rättigheter, när det är lämpligt. Samordningsuppdraget innefattar även att bistå personuppgiftsansvariga nämnder med samordning och stöd vid konsekvensbedömning.

3. Dataskyddsombud och dataskyddskontakter

Varje nämnd, bolag och stiftelse ska utnämna ett dataskyddsombud (se artikel 37-39 GDPR). Nämndernas förvaltningar samt bolag och stiftelse rekommenderas därutöver att utse dataskyddskontakter som löpande arbetar med att verksamheten ska leva upp till de krav som ställs i GDPR.

3.1 Dataskyddsombudets roll

Dataskyddsombudets uppgift är att informera och ge råd till de personuppgiftsansvariga verksamheterna kring vilka skyldigheter som gäller enligt GDPR och kompletterande nationella bestämmelser. Dataskyddsombudet ska också bevaka att reglerna följs och rapportera till den personuppgiftsansvarige.

Kommunens dataskyddsombud är placerat centralt på kommunstyrelsens förvaltning men arbetar på uppdrag av respektive nämnd, bolag och stiftelse som utsett kommunens dataskyddsombud som dataskyddsombud för sin verksamhet.

3.2 Dataskyddskontakternas roll

Dataskyddskontakternas löpande arbete ska åtminstone omfatta följande.

1. Upprätta och underhålla förteckning över personuppgiftsbehandlingen i enlighet med vad som stadgas i artikel 30.1-3 GDPR.

2. Samordna och besvara begäranden från registrerade för den egna verksamheten, såsom exempelvis begäran om registerutdrag, radering och invändning. (Se artikel 12-22 GDPR.)

3. Säkerställa att nödvändiga rutiner och instruktioner finns tillgängliga inom den egna verksamheten så att behandlingen sker i enlighet med de grundläggande principerna i artikel 5.1.

4. Vara behjälplig med att bedöma om personuppgiftsincidenter ska vidarerapporteras till **Integritetsskyddsmyndigheten** (IMY) och om de registrerade ska informeras. (Se artikel 33.1 och artikel 34 GDPR.)

5. Vara förvaltningens, bolagets eller stiftelsens representant i det kommunövergripande nätverket för dataskyddskontakter.

6. Vara ett stöd till personuppgiftsansvarig, förvaltnings- eller bolagsledningen och verksamheten i arbetet med personuppgiftsfrågor.

7. Uppmärksamma personuppgiftsansvarig och förvaltnings- eller bolagsledning på åtgärder som måste vidtas för att upprätthålla en god hantering av personuppgifter i enlighet med gällande lagstiftning.

8. Vara dataskyddsombudet behjälplig samt fungera som länk mellan dataskyddsombudet och personuppgiftsansvarig

9. Omvärldsbevaka kring personuppgiftsfrågor utifrån det egna verksamhetsområdet.

10. Vid behov inhämta råd och stöd från dataskyddsombudet, till exempel vid konsekvensbedömning avseende dataskydd i enlighet med artikel 35.2 samt 39.1 c GDPR.

4. Krav på digitala tjänster och system som medför behandling av personuppgifter

För varje digital tjänst och system som används, eller som det finns planer på att använda, ska det särskilt beaktas om användandet kan komma att medföra behandling av personuppgifter. För det fall personuppgifter kommer att behandlas ska det säkerställas att det finns förutsättningar för såväl den som är personuppgiftsansvarig som för dess personuppgiftsbiträde att kunna fullgöra sina skyldigheter avseende dataskydd.

Vid inköp och upphandling av digitala tjänster och verksamhetssystem som kan komma att användas för behandling av personuppgifter ska krav ställas på att lösningen lever upp till kraven i GDPR och nationella bestämmelser på dataskyddsområdet. Kraven ska utformas i samråd mellan kommunens upphandlingsfunktion och den eller de nämnder som är personuppgiftsansvariga, alternativt den nämnd som har samordningsuppdrag för den aktuella behandlingen.

5. Konsekvensbedömning avseende dataskydd

Om en typ av behandling kan komma att leda till hög risk för registrerades rättigheter och friheter ska en bedömning av den planerade behandlingens risker och konsekvenser göras i syfte att sänka riskerna eller undvika behandlingen (se artikel 35–36). Konsekvensbedömningen ska utföras av den nämnd, bolag eller stiftelse som är personuppgiftsansvarig. Om en annan nämnd har samordningsuppdrag ska denna bistå med den samordning som behövs för bedömningen. Beslut om personuppgiftsbehandlingen ska dock alltid fattas av den personuppgiftsansvarige.

Dataskyddsombudet ska involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling som innebär hög risk för registrerade kan komma ifråga.

6. Incidentrapportering

Varje nämnd, bolag och stiftelse ska ha rutiner för att kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten inom 72 timmar från upptäckt på det sätt som anges i artikel 33 och 34 i GDPR. Rapportering till tillsynsmyndigheten behöver emellertid inte göras om det är osannolikt att incidenten kan komma att medföra en risk för de registrerades rättigheter och friheter.

En nämnd som agerar personuppgiftsbiträde ska – istället för att rapportera till tillsynsmyndigheten inom 72 timmar – underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident. Om möjligt ska underrättelse ske samma dag. Personuppgiftsbiträdet ska också i övrigt bistå personuppgiftsansvarig på det sätt som följer av *Regler för interna personuppgiftsbiträdesförhållanden inom Kungsbacka kommun*.

Den nämnd som har samordningsuppdrag ska vid behov därtill bistå med samordning i hanteringen av incidenter som berör flera verksamheter i samråd med de nämnder som är berörda såsom personuppgiftsansvariga.

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

Kommunstyrelsens förvaltning ska samordna en uppföljning av personuppgiftsincidenter inom kommunen i syfte att sprida lärdom och förebygga att incidenter upprepas.

7. Förteckning över personuppgiftsbehandlingar

Varje nämnd, bolag och stiftelse ska löpande föra en förteckning över vilka personuppgifter som behandlas i den egna verksamheteten (se artikel 30). Kommunstyrelsens förvaltning ska samordna arbetet i syfte att främja likvärdighet och överblickbarhet i kommunens personuppgiftsbehandling.

Behandlingar som berör flera nämnder ska förtecknas av den nämnd som har samordningsuppdraget för behandlingen och noteras i respektive personuppgiftsansvarigs förteckning. Behandling som utförs för en annan nämnds räkning ska, utöver den personuppgiftsansvarigas förteckning, även förtecknas i personuppgiftsbiträdesnämndens behandlingsförteckning.

8. Personuppgiftsbiträdesförhållanden

8.1 Extern part

Varje nämnd ska teckna personuppgiftsbiträdesavtal (PUB-avtal) när denne uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter för de digitala verktyg och system som nämnden är ensam användare av.

För att en nämnd som agerar personuppgiftsbiträde ska kunna teckna underbiträdesavtal med en extern part krävs att den personuppgiftsansvarige nämndens instruktion inte hindrar det. Om behandlingen avser personuppgifter för flera olika personuppgiftsansvariga nämnder krävs att ingen av dessa nämnders instruktioner hindrar att biträdet anlitar underbiträde. Se vidare 8.2.

Varje bolag och stiftelse ska teckna PUB-avtal med de parter som de uppdrar att behandla personuppgifter för dess räkning.

Innan personuppgiftsbehandlingar läggs över på en extern part ska det kontrolleras att speciallagstiftning gällande personuppgiftsbehandlingen inte hindrar det.

8.2 Mellan kommunens nämnder

Eftersom det inte är möjligt för kommunala nämnder att teckna civilrättsligt bindande avtal med andra nämnder inom samma kommun måste förhållandet i stället regleras i en så kallad rättsakt (se artikel 28.3 GDPR). *Regler för interna personuppgiftsbiträdesförhållanden inom Kungsbacka kommun* kompletterar denna riktlinje och ska kompletteras med en instruktion från den personuppgiftsansvariga nämnden till biträdesnämnden. Reglerna tillsammans med instruktionen för behandlingen utgör en sådan rättsakt som avses i GDPR.

När personuppgiftsbehandlingar läggs över från en nämnd till en annan nämnd ska det även kontrolleras om personuppgiftsbehandlingarna styrs av speciallagstiftning eller myndighetsutövning som medger att de kan hanteras av en annan nämnd såsom biträde.

Kommunstyrelsens förvaltning ska administrera en dokumentmall för den instruktion som reglerna för biträdesförhållandet ska kompletteras med från den personuppgiftsansvariga nämnden till biträdesnämnden.

Nämnderna ska ha en sammanställning över de instruktioner som reglerar deras biträdesrelationer med interna parter.

9. Överenskommelse vid gemensamt personuppgiftsansvar

När två personuppgiftsansvariga använder och kan besluta om ändamål och medel för behandlingen av personuppgifter i ett och samma system föreligger ett gemensamt personuppgiftsansvar. Gemensamt personuppgiftsansvar kan finnas med en extern personuppgiftsansvarig part (exempelvis en extern utförare av kärnverksamhet) eller en intern part (exempelvis folkbibliotek respektive skolbibliotek där två nämnder använder uppgifter ur samma system för varsitt ändamål). I dessa fall ska det tecknas en överenskommelse där de personuppgiftsansvarigas respektive ansvar för att fullgöra skyldigheterna enligt GDPR och andra nationella dataskyddsbestämmelser fastställs (se artikel 26 GDPR).

Kommunstyrelsens förvaltning ansvarar för att tillhandahålla en dokumentmall för de villkor som ska gälla vid gemensamt personuppgiftsansvar mellan två eller flera nämnder.

Nämnderna, bolagen och stiftelsen ska ha en sammanställning över aktuella avtal som reglerar deras gemensamma personuppgiftsansvar med externa och interna parter.

10. Information till de registrerade

Kommunstyrelsens förvaltning ska ta fram och tillhandahålla övergripande information om kommunens personuppgiftsbehandling och de registrerades rättigheter i syfte att underlätta för de personuppgifts-ansvariga inom kommunen att uppfylla kraven i artikel 12 i GDPR.

Varje nämnd, bolag och stiftelse ska därutöver ha rutiner för hur information till registrerade ska tillhandahållas utifrån den behandling som utförs inom dess verksamhetsområde i enlighet med kraven i artikel 12-14 i GDPR.

11. Tillgång, rättelse, radering, begränsning, flytt av personuppgifter, invändning och klagomål

Kommunstyrelsens förvaltning ska samordna kommunens rutiner för hanteringen av begäranden från registrerade om att utöva sina rättigheter i artikel 15-22 i GDPR, vilket bland annat innebär att

- Få tillgång till information om sina personuppgifter
- Rätta eller komplettera sina uppgifter
- Radera sina uppgifter
- Begränsa sina uppgifter
- Utnyttja möjligheten till dataportabilitet om sådan möjlighet finns
- Invända mot behandlingen.

Beslutad av: Kommunstyrelsen 19 oktober 2021 § 278 och
Kommunfullmäktige 9 november 2021 § 142, KS 2021-00691

Gäller från: 9 november 2021

Ansvarig förvaltning: Kommunstyrelsens förvaltning

Kontakt: Kungsbacka direkt 0300-83 40 00, info@kungsbacka.se

Kungsbacka kommun, 434 81 Kungsbacka
kungsbacka.se