



ÖCKERÖ KOMMUN

Beslutsdatum:	2018-08-28
Beslutande:	Kommunstyrelsen
Giltighetstid:	Tillsvidare
Dokumentansvarig:	Kommundirektör
Upprättad av:	Anna Corneliusson, verksamhetsutvecklare

RIKTLINJER FÖR HANTERING AV PERSONUPPGIFTER I ÖCKERÖ KOMMUN

EU:s dataskyddsförordning (2016/679) och den svenska Dataskyddslagen (2017/18) innehåller regler för hur personuppgifter får behandlas. Personuppgifter är uppgifter och information som kan kopplas till en fysisk person som är i livet. Lagstiftningen beskriver hur man får behandla personuppgifter, med stöd av lag eller avtal, i myndighetsutövning eller med stöd av samtycke från den registrerade. Lagstiftningen gäller all behandling, eller hantering, av personuppgifter. Oavsett om den sker digitalt eller manuellt.

I Öckerö kommun hanteras en mängd personuppgifter. Dessa riktlinjer beskriver hur Öckerö kommun ska säkerställa att dataskyddslagstiftningen efterlevs. Riktlinjerna omfattar samtliga nämnder i Öckerö kommun och utgör ett komplement till *Policy för hantering av personuppgifter* samt den lagstiftning som reglerar behandling av personuppgifter. Riktlinjerna anger ansvarfördelning och vad verksamheterna behöver tänka på när personuppgifter hanteras. De kompletteras med rutiner och instruktioner som på ett mer detaljerat sätt stödjer verksamheterna i konkreta process- och hanteringsfrågor.

PERSONUPPGIFTSHANTERING

Ur policyn för hantering av personuppgifter

I Öckerö kommun ska all hantering av personuppgifter ske med den enskildes integritet i fokus. Följande principer ska alltid följas:

- *Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning*
- *Behandlingen ska vara laglig, korrekt och öppen gentemot den registrerade*
- *Innan behandling påbörjas ska ett särskilt och uttryckt ändamål vara fastställt*
- *Endast de personuppgifter som är nödvändiga för ändamålet ska samlas in*

- *Åtkomst till personuppgifter ska begränsas till de som är behöriga*
- *Personuppgifter ska inte sparas längre än vad som är nödvändigt för ändamålet, om inte lag anger annat*

Varje nämnd ska se till att medarbetarna har tillräcklig kunskap om ovanstående principer så att de följs vid all behandling av personuppgifter i verksamheten.

ORGANISATORISKA OCH TEKNISKA FÖRUTSÄTTNINGAR

Ur policyn för hantering av personuppgifter

Öckerö kommun ska vid planering av olika verksamheter säkerställa att det ges såväl organisatoriska som tekniska förutsättningar att uppfylla de krav som gäller enligt dataskyddslagstiftning.

Varje nämnd eller styrelse är personuppgiftsansvarig för de personuppgifter som behandlas inom nämndens ansvarsområde och verksamhet. Varje nämnd ska säkerställa att det finns såväl organisatoriska som tekniska förutsättningar inom den egna förvaltningen eller verksamheten för att uppfylla de krav som ställs på personuppgiftsansvariga i dataskyddslagstiftningen.

Organisation och kompetens

Varje förvaltning och verksamhet ska ha rätt resurser och relevant kompetens inom området för att kunna följa lagstiftningen samt dessa riktlinjer. Varje förvaltningen bör ha minst en person i verksamheten, en så kallad personuppgiftskontakt, som är utsedd att vara kontaktperson gentemot Kommunstyrelsens enhet för kansli och juridik.

Enheten för kansli och juridik ska vara samordnare för förvaltningarnas personuppgiftskontakter och vara den centrala kontakten gentemot dataskyddsbudet.

Dataskyddsbud

Varje nämnd ska utnämna ett dataskyddsbud som ska rapportera direkt till förvaltningsledningen. Dataskyddsbudet ska utses på grundval av sina yrkesmässiga kvalifikationer och ska ha god kunskap om dataskyddslagstiftningen och gällande praxis. Efter att dataskyddsbudet är utsett ska det anmälas till tillsynsmyndigheten.

Öckerö kommun har tillsammans med Partille, Härryda och Lerums kommun samt Göteborgsregionens kommunalförbund (GR) tecknat ett samverkansavtal för ett gemensamt dataskyddsbud. Det gemensamma dataskyddsbudet utses för samtliga nämnder i Öckerö kommun.

Förvaltningsledningen ska säkerställa att dataskyddsbudet involveras och rådfrågas på ett tidigt stadium när ny behandling av personuppgifter kan komma ifråga. Förvaltningen ska även informera dataskyddsbudet vid rapportering av personuppgiftsincidenter. Dataskyddsbudet ska vid begäran få tillgång till dokumentation och uppgifter som hen behöver för att kunna granska förvaltningens arbete.

Dataskyddsbudet ska, enligt samverkansavtalet, bland annat:

- Vara ett kunskapsstöd, informera och ge råd till parterna om innehåll och tillämplighet av gällande dataskyddsskyddslagstiftning och angränsande regler som aktualiseras,
- fungera som kontaktpunkt för och mellan tillsynsmyndigheten, och vid behov genomföra förhandssamråd,
- rapportera till kommunens ledning angående dataskyddsfrågor, organisatoriska brister och utvecklingsbehov och liknande frågor, när så är påkallat,
- arbeta för organisatoriska säkerhetsskyddsåtgärder,
- identifiera kompetensutvecklingsbehov, planera och genomföra utbildningar avseende dataskyddslagstiftningen samt övervaka den interna efterlevnaden av organisationens riktlinjer för dataskydd,
- bistå i utredningen av misstänkta dataintrång,

- ge råd vid genomförande av konsekvensbedömning av dataskydd och övervaka genomförande av denna,
- omvärldsbevaka frågor rörande dataskyddslagstiftningen,
- övervaka den interna efterlevnaden av dataskyddslagstiftningen.

Inköp och upphandling

Vid inköp och upphandling av tjänster, produkter och applikationer som kan komma att leda till behandling av personuppgifter ska verksamheten ställa krav på att tjänsten eller produkten lever upp till kraven i dataskyddslagstiftningen.

Vid utredning av vilka säkerhetskrav som bör ställas ska, vid behov, samråd ske med Enheten för digitalisering och kommunikation.

Vid inköp och upphandling av produkter, tjänster och applikationer som är baserade på behandling av personuppgifter bör urvalet, när det är lämpligt, utformas på ett sätt som ger ett incitament för anbudsgivare att driva på utvecklingen enligt principerna om inbyggt dataskydd (privacy by design) och dataskydd som standard (privacy by default).

Konsekvensbedömning

När en ny typ av behandling av personuppgifter kan komma att leda till att registrerades rättigheter och friheter riskeras ska en bedömning av den planerade behandlingens konsekvenser utföras.

Verksamheterna ansvarar för att anmäla den nya behandlingen till kommunens registerförteckning och enheten för kansli och juridik ansvarar för att genomföra en riskbedömning i syfte att avgöra om en konsekvensbedömning behöver göras. Konsekvensbedömning ska ske i samråd med dataskyddsombudet.

Incidentrapportering

Varje förvaltningen ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten. En personuppgiftsincident ska anmälas till tillsynsmyndigheten inom 72 timmar från det att händelsen har upptäckts. Rapportering av personuppgiftsincidenter ska ske enligt den kommunövergripande rutinen för rapportering av personuppgiftsincidenter.

Säkerhet i samband med behandlingen

Varje nämnd ansvarar för att en lämplig säkerhetsnivå finns vid behandling av personuppgifter. Förvaltningen eller verksamheten ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå utifrån de kriterier som anges i dataskyddslagstiftningen.

Vid planering av verksamheten ska särskild hänsyn tas till att personuppgifter inte behandlas i högre utsträckning eller under längre tid än vad som är nödvändigt. Åtkomst till personuppgifter ska begränsas till de som behöver dem för att kunna utföra sitt arbete.

Anställda som på något sätt kan komma att behandla personuppgifter i sitt arbete ska genomgå utbildning för att säkra att personuppgifter hanteras på ett lagligt och respektfullt sätt.

KONTROLL ÖVER PERSONUPPGIFTSBEHANDLINGAR

Ur policyn för hantering av personuppgifter

Öckerö kommun ska ha kontroll över verksamhetens behandling av personuppgifter.

Kommunstyrelsen ska definiera ansvaret mellan kommunstyrelsen och övriga nämnder för de personuppgifterbehandlingar som sker för en annan nämnds räkning eller då det föreligger ett gemensamt personuppgiftsansvar.

Register över personuppgiftsbehandlingar

Varje nämnd ska föra ett register över vilka personuppgifter som behandlas i den egna verksamheten. Registret ska följa centralt framtagna instruktioner och årligen ses över och uppdateras på uppmaning från enheten för kansli och juridik. Enheten för kansli och juridik ska säkerställa att kommunens register är korrekta och följer dataskyddsförordningens krav.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar

När en nämnd anlitar en extern part att behandla personuppgifter ska nämnden säkerställa att den externa kan ge tillräckliga garantier om att skydda de personuppgifter den får tillgång till. Detta ska säkerställas genom ett personuppgiftsbiträdesavtal (PUB-avtal). Verksamheterna ska ange i registerförteckningen att personuppgiftsbiträdesavtal finns upprättat.

I de fall där det finns ett gemensamt personuppgiftsansvar med en extern part ska nämnden se till att det tecknas ett avtal där de personuppgiftsansvarigas respektive ansvar för att fullgöra skyldigheterna enligt dataskyddslagstiftningen beskrivs och fastställs.

Kommunstyrelsen ska administrera en förteckning över ansvarsfördelningen mellan Öckerö kommuns nämnder (inklusive kommunstyrelsen) för de personuppgifter som behandlas för en annan nämnd, alternativt då det finns ett gemensamt personuppgiftsansvar mellan två eller flera nämnder.

REGISTRERADES RÄTTIGHETER

Ur policyn för hantering av personuppgifter

Öckerö kommun ska vara tillmötesgående och förberedd på att hjälpa de registrerade att tillvarata sina rättigheter enligt dataskyddslagstiftningen.

Information till de registrerade

Varje förvaltning ansvarar för att information ges till de registrerade för de specifika personuppgiftsbehandlingar som sker inom deras ansvarsområde.

Tillgång, rättelse, radering och begränsning

Varje förvaltning ska ha rutiner för hantering av begäranden från registrerade om att utöva sina rättigheter att:

- Rätta eller komplettera sina uppgifter,
- radera sina uppgifter,
- begränsa sina uppgifter,
- utnyttja möjligheten till dataportabilitet om sådan möjlighet finns.

Registerutdrag

Kommunstyrelsen ska ta emot och administrera begäran om registerutdrag. Varje förvaltning ska på uppmaning från enheten för kansli och juridik tillhandahålla den information som de efterfrågar.

PERSONUPPGIFTSANSVAR OCH SAMORDNANDE ANSVAR

Ur policyn för hantering av personuppgifter

Varje nämnd är personuppgiftsansvarig och ansvarar för den hantering av personuppgifter som sker inom nämndens verksamhet och ansvarsområde.

Kommunstyrelsen ska leda, samordna och stödja verksamheternas arbete med att uppfylla kraven i dataskyddslagstiftningen. Kommunstyrelsen ska vid behov utfärda kompletterande riktlinjer för behandling av personuppgifter samt ta fram mer detaljerade rutiner, mallar och annat underlag som underlättar de personuppgiftsansvarigas fullgörande av sitt ansvar. Detta stöd innefattar inte någon inskränkning eller begränsning av respektive personuppgiftsansvarigs ansvar.

Kommunstyrelsen genom enheten för kansli och juridik har till uppgift att ansvara för kommunens registerförteckningar samt stödja kommunens förvaltningar i deras arbete att efterleva bestämmelserna i dataskyddslagstiftningen (KS § 112/18).

Kommunstyrelsens samordnande ansvar

I stycken ovan anges att enheten för kansli och juridik ska vara samordnare för förvaltningarnas personuppgiftskontakter samt kontakt gentemot dataskyddsombudet, ansvara för rutiner för

personuppgiftsincident och konsekvensbedömning, ansvara för kommunens registerförteckningar, administrera en förteckning över de behandlingar som sker för en annan nämnd eller då det finns ett gemensamt personuppgiftsansvar samt ta emot och administrera begäran om registerutdrag.

Enheten ska även:

- hålla information om kommunens hantering av personuppgifter uppdaterad på kommunens webbplats,
- hålla kontaktuppgifter till nämndernas dataskyddsombud uppdaterade på webbplatsen samt vid förändringar meddela detta till tillsynsmyndigheten,
- ansvara för den interna informationen på kommunens intranät,
- identifiera generella hanteringssvårigheter och problem i verksamheterna och ta fram stödmaterial för detta,
- svara på frågor samt vid behov ta hjälp av dataskyddsombudet för att kunna ge svar,
- vara systemägare för kommunens system för registerförteckningar.