Kommunfullmäktige
Lina Johannesson, 0573-141 26
lina.johannesson@arjang.se

RIKTLINJE

Datum
2018-04-27

Diarienummer
Dnr KS 2018/210.00

Antagen av
Kommunfullmäktige

Paragraf
2018-06-18 § 96

Riktlinjer för behandling av personuppgifter i Årjängs kommun

Sammanfattning

Detta dokument reglerar hur Årjängs kommun behandlar personuppgifter i enlighet med reglerna i dataskyddsförordningen (GDPR).

Dokumentet omfattar både kommunen och dess bolag. När Årjängs kommun och/eller kommunen benämns i dokumentet innefattar den benämningen även kommunens helägda bolag.

Innehåll

1 Bakgrund

EU:s dataskyddsförordning börjar tillämpas 25 maj 2018. Förordningen kommer att gälla som lag i Sverige och ersätter personuppgiftslagen (1998:204). Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU.

Dataskyddsförordningen (GDPR) har till syfte att skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av deras personuppgifter.

Dataskyddsförordningen innehåller generella regler och strider inte mot övriga lagar angående behandling av personuppgifter. Den 25 maj träder även den svenska dataskyddslagen (prop. 2017/18:105) i kraft, som innehåller kompletterande bestämmelser till dataskyddsförordningen.

1.1 Sanktioner

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att behandlingen är samt att de sex principer följs för behandling av personuppgifter, vilket medför ökade krav på dokumentation om hur organisationen efterlever förordningens regler.

Det kommer att införas möjligheter för tillsynsmyndigheten (Datainspektionen) att utdöma en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter.

1.2 Dokumentation

Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt man följer dem. Det finns flera sätt att visa detta, till exempel genom att ha tydlig information till de registrerade, att dokumentera de behandlingar som pågår i organisationen och de överväganden man har gjort, samt att ha dokumenterade interna riktlinjer för dataskyddet (detta dokument).

2 Definitioner

2.1 Personuppgift

En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Det kan även uttryckas som så att en person är identifierbar eller sökbar utifrån de uppgifter som förs.

2.2 Behandling

En behandling av personuppgifter omfattar varje åtgärd som vidtas i fråga om personuppgifter. Begreppet är teknikneutralt vilket innebär att det kan handla om manuell eller automatiserad/datoriserad behandling. Det kan enligt förordningen vara fråga om insamling, registrering, organisering, lagring, bearbetning eller ändring, utlämnande, utplåning eller förstöring, sammanställning eller samkörning etc.

2.3 Personuppgiftsansvarig

Personuppgiftsansvarig är den som ensam eller tillsammans med annan bestämmer ändamålen med och/eller medlen för behandling av personuppgifter. I kommunkoncernen är det kommunstyrelsen och ansvariga nämnder i egenskap av självständiga förvaltningsmyndigheter samt de kommunala bolagens styrelser.

2.4 Dataskyddsombud

De personuppgiftsansvariga i kommunkoncernen har skyldighet att utse ett dataskyddsombud. Ombudet ska informera, ge råd och övervaka efterlevnaden av förordningen samt samarbeta med tillsynsmyndigheten.

2.5 Personuppgiftskontaktperson

Kontaktpersonerna är en eller flera personer som inom respektive verksamhet/bolag ansvarar för det praktiska dataskyddsarbetet, till exempel att ansvara för att registerförteckningar förs över samtliga personuppgiftsbehandlingar.

2.6 Personuppgiftsbiträde

Personuppgiftsbiträde avser såväl en fysisk som juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning. Endast personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

2.7 Personuppgiftsbiträdesavtal

När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett biträdesavtal.

2.8 Den registrerade

Den registrerade är den person som en personuppgift avser.

3 Behandling av personuppgifter

3.1 Rättslig grund

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Grundläggande principer inom dataskydd är att inte samla in mer information än vad som behövs, inte ha kvar information längre än nödvändigt och inte använda uppgifter till något annat än vad som var syftet när de samlades in.

Har den registrerade lämnat sitt samtycke till behandling av personuppgifterna är behandling i regel tillåten. Ett samtycke skall vara individuellt, frivilligt, tydligt och informerat efter det att den registrerade fått information om tilltänkt behandling.

Den registrerade kan när som helst återkalla sitt samtycke vartefter behandling inte vidare kan ske.

Samtycke ska endast användas i undantagsfall som laglig grund i kommunens verksamhet. För kommunens verksamhet ska någon av följande lagliga grunder användas för behandling av personuppgifter:

- Avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas.
- Personuppgiftsansvarige skall kunna fullgöra en rättslig förpliktelse
- Skydda vitala intressen för den registrerade
- En arbetsuppgift av allmänt intresse skall kunna utföras
- Utföra en arbetsuppgift i samband med myndighetutövning
- Utföra arbetsuppgifter som är nödvändiga för ändamål som rör den personuppgiftsansvariges berättiga intressen. (Det är fortfarande inte helt klarlagt i vilken utsträckning kommuner (myndigheter) kommer att kunna utnyttja denna grund för att hantera personuppgifter)

3.1.1 Personuppgifter på kommunens/bolagens hemsidor

Behandling av personuppgifter på hemsidan är tillåten om det finns ett allmänt intresse av att publicera uppgiften eller om samtycke finns.

Fotografier på identifierbara personer kräver samtycke av den registrerade om det inte finns ett allmänt intresse av att bilden publiceras.

Personuppgifter (dock ej personnummer, se punkt 3.3.1) som ingår i ett justerat protokoll som förts vid ett nämnd-, styrelse-, eller fullmäktigesammanträde får publiceras på kommunens/bolagens hemsida. Innan materialet läggs ut på hemsidan skall det granskas så att inga integritetskänsliga eller sekretessbelagda personuppgifter publiceras.

3.1.2 Offentlighetsprincipen

Offentlighetsprincipen innefattar en rätt för var och en att hos myndigheter ta del av allmänna handlingar. Denna rätt gäller dock inte om handlingarna innehåller uppgifter för vilka gäller sekretess enligt offentlighets- och sekretesslagen. Enligt den gäller exempelvis sekretess för personuppgift om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med dataskyddsförordningen.

3.2 Särskilt om känsliga personuppgifter

Särskilda regler finns för behandling av känsliga personuppgifter (personuppgifter av särskild karaktär).

Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter.

Känsliga personuppgifter är uppgifter som avslöjar:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiösa eller filosofiska övertygelser
- Medlemskap i fackförening
- Uppgifter som rör sexualitet och hälsa
- Genetiska och biometriska uppgifter.

Ett antal undantag finns i artikel 9 i förordningen där det anges när verksamheten får behandla känsliga personuppgifter, till exempel om det finns ett uttryckligt samtycke.

I Årjängs kommun ska känsliga personuppgifter endast behandlas när det finns särskilt stöd i lag eller om den registrerade särskilt samtyckt till den specifika behandlingen.

Det här innebär att varje gång känsliga personuppgifter ska användas av Årjängs kommun måste en särskild bedömning ske om att hanteringen verkligen är tillåten och att den sker på ett säkert sätt. Känsliga personuppgifter ska alltid ges ett högt skydd mot obehörig åtkomst.

3.3 Särskilt om extra skyddsvärda personuppgifter

Även personuppgifter som inte är särskilt reglerade som känsliga kan de vara mer skyddsvärda än andra. Personuppgifter av mycket personlig eller privat natur anses generellt vara mer skyddsvärda än andra typer av personuppgifter. Så gör även personuppgifter som möjliggör samkörning mellan register som t.ex. personnummer eller andra samordningsnummer.

Det här innebär att kommunen alltid ska bedöma om de personuppgifter som behandlas är särskilt skyddsvärda mot bakgrund till sin privata natur, sin mängd eller av annan anledning. Denna bedömning har betydelse för valet av nivå för skyddsåtgärder.

3.3.1 Personnummer

Personnummer och samordningsnummer ska enligt dataskyddslagen endast hanteras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Det här innebär att kommunen alltid ska bedöma om personnummer är en nödvändig del av en behandling av personuppgifter och alltid överväga om ändamålen kan uppfyllas utan att personnummer används.

3.4 Särskilt om behandling av personuppgifter i hälso- och sjukvården

När personuppgifter behandlas inom hälso- och sjukvården ska Patientdatalagen (2008:355) samt Socialstyrelsens föreskrift HSLF-FS

2016:40 Journalföring och behandling av personuppgifter i hälso- och sjukvården tillämpas på dess hantering.

Enligt 3 kap. 5 § HSLF-FS 2016:40 ska kommunen som vårdgivare utföra riskanalyser om en behandling av personuppgifter inom verksamheten riskerar att inte uppfylla kraven som ställs på behandlingen enligt föreskriften. Riskanalyserna ska dokumenteras.

Socialstyrelsen ställer även andra grundläggande krav på behandlingen av uppgifter bland annat att all överföring och åtkomst till personuppgifter om patienter som sker över öppna nät ska ske på ett säkert sätt med insynsskydd och stark autentisering av mottagare och avsändare.

4 Informationskravet och de registrerades rättigheter

4.1 Klar och tydlig information

Vid insamlande av personuppgifter ska den registrerade ges information om behandlingen.

Vid insamlande av personuppgifter måste enligt dataskyddsförordningen lämnas viss information, exempelvis

- identitet (vem är det som kräver in personuppgifter?)
- ändamål med behandlingen (vad ska uppgifterna användas till)
- rättsliga grunder för behandlingen
- hur länge personuppgifterna lagras
- möjligheten att lämna klagomål till tillsynsmyndigheten om man anser att ens personuppgifter har hanterats felaktigt

Informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk. Enligt förordningen förtjänar barn (under 16 år) särskilt skydd vilket gör att information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt som barn förstår.

4.2 Rättigheter för den registrerade

4.2.1 Den registrerades rätt till information om personuppgifterna som behandlas

Den registrerade har rätt att få veta bland annat vilket ändamål behandlingen avser och hur länge uppgifterna sparas, s k registerutdrag.

4.2.2 Rätt till rättelse av uppgifterna

Kommunen och dess bolag ska under alla omständigheter se till att uppgifterna är korrekta. Om personuppgifterna är felaktiga har den registrerade rätt att begära rättelse.

4.2.3 Få sina personuppgifter raderade

Beroende på omständigheter i det enskilda fallet och vilken rättslig grund som personuppgiftsbehandlingen görs kan den registrerade även ha rätt till radering av sina personuppgifter. Rättigheten har begränsad tillämpning inom offentlig förvaltning eftersom merparten av personuppgiftsbehandlingarna vilar på en rättslig grund där rättigheten inte är tillämplig.

4.2.4 Rätt till dataportabilitet

Den registrerade har rätt att få ut de uppgifter som rör honom eller henne samt få dem överförda till en annan personuppgiftsansvarig i den mån det är tekniskt möjligt.

4.2.5 Information till den registrerade om personuppgiftsincident

Personuppgiftsincidenter (dataintrång) ska anmälas till Datainspektionen inom 72 timmar från det att händelsen upptäcks. Om intrånget har lett till allvarliga risker för den registrerade ska den registrerade kontaktas.

4.2.6 Information till barn

Barn förtjänar ett särskilt skydd enligt dataskyddsförordningen.

Den information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt.

5 Kommunen (de personuppgiftsansvarigas) ansvar

Kommunens ansvar i enlighet med dataskyddsförordningen kan sammanfattas med att kommunstyrelsen samt nämnder och bolagens styrelser, i egenskap av personuppgiftsansvariga, behöver ha kännedom om var personuppgifter behandlas och att det dokumenteras. Den som är personuppgiftsansvarig måste kunna visa att förordningens regler följs.

5.1 Registerförteckning

Dokumentation som på något sätt behandlar personuppgifter ska sammanställas i en registerförteckning. Även ostrukturerat material ska ingå i denna förteckning. Personuppgiftskontaktpersonen inom respektive verksamhet/bolag ansvarar för att koordinera detta arbete.

5.2 Risk- och konsekvensbedömning

Vid dokumentation av personuppgifter ska vid upprättande av registerförteckning en första bedömning genomföras för att värdera risken och allvaret om uppgifter skulle spridas. Resultatet av bedömningen ska beaktas då lämpliga åtgärder fastställs. Konsekvenserna bedöms av kommunen som hög i och med att vi behandlar personuppgifter av särskild karaktär (känsliga personuppgifter) vilket alltid påkallar en risk- och konsekvensbedömning där dataskyddsombudet (DSO) alltid ska rådfrågas. Det kan vara aktuellt med samråd med tillsynsmyndigheten om inte säkerheten kan garanteras.

Gällande principer är att inte samla in mer information än vad som är nödvändigt, inte ha kvar informationen längre än nödvändigt samt att inte använda uppgifterna till annat än till angivet syfte. Det är viktigt att beakta möjligheten att minimera tillgång till uppgifterna.

5.3 Säkerhet

Grundskyddet att information, och därmed även personuppgifter, behandlas korrekt är att endast personer som behöver åtkomst till uppgifterna för att kunna utföra sitt arbete har åtkomst till personuppgifterna. Rutiner för åtkomst och behörighet ska finnas dokumenterade till varje register eller system där personuppgifter behandlas. Detta gäller oavsett vilken typ av personuppgifter som behandlas. Utöver detta ska kontroll av behörigheter kontrolleras regelbundet så att det endast är behöriga användare som har åtkomst till personuppgifterna.

Personuppgifter som behandlas inom vård- och omsorg ska även beakta särskilda säkerhetskrav utifrån specifik särlagstiftning, inte minst med avseende på åtkomst och behörigheter samt loggningskrav (patientdatalagen).

Om behandlingen avser personuppgifter som är integritetskänsliga, eller personuppgifter av särskild karaktär, ska dessutom loggning ske av:

- Vem som loggar på
- Vilka uppgifter som behandlats
- Tidpunkt för behandling

Personuppgifter av särskild karaktär samt integritetskänsliga personuppgifter som kan nås över öppna nätverk ska beaktas särskilt avseende säker

överföring samt påloggning. För att säkerställa en säker behandling av dess uppgifter som kan nås över öppna nätverk ska en risk- och konsekvensbedömning genomföras i samråd med dataskyddsombudet (DSO).

5.4 Användande av personuppgiftsbiträde

De personuppgiftsansvariga ska endast använda sig av personuppgiftsbiträde för sin behandling av personuppgifter om det anlitade personuppgiftsbiträdet ger tillräckliga garantier om skydda personuppgifter genom såväl tekniska som organisatoriska åtgärder. Nivån på skyddet ska överensstämma med den nivå som enligt kommunens bedömning krävs för att behandlingen ska uppfylla dataskyddsförordningens krav och för att säkerställa att de registrerades rättigheter skyddas.

Personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde (s.k. underbiträde) utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits från kommunen. Om ett sådant allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet löpande informera kommunen om eventuella planer på att anlita eller ersätta personuppgiftsbiträden, så att kommunen har möjlighet att göra invändningar.

När personuppgiftsombud anlitas ska ett biträdesavtal (PUB-avtal) tecknas mellan biträdet och kommunen. Avtalet ska som huvudregel följa kommunens mall för biträdesavtal. Undantag från denna huvudregel ska endast ske efter att en bedömning skett om att föreslaget biträdesavtal uppfyller dataskyddsförordningens och kommunens krav.

Biträdesavtalet ska undertecknas av den som enligt gällande delegationsordning har ansvaret att underteckna det tjänsteavtal som biträdesavtalet utgör en bilaga till.

5.5 Överföring av personuppgifter utanför EU/EES

Huvudregeln är att ett förbud råder mot att föra ut personuppgifter utanför EU/EES.

Enligt dataskyddsförordningen är överföring av personuppgifter utanför EU/EES endast tillåtet under vissa omständigheter. För överföring av personuppgifter till ett land utanför EU/EES krävs att landet uppfyller dataskyddsförordningens och EU-kommissionens krav på s.k. adekvat skyddsnivå för personuppgifter eller att EU-kommissionens standardavtalsvillkor används vid avtalsskrivandet med leverantören. För överföring av personuppgifter till USA kan det annars räcka att den mottagande leverantören är anslutet till villkoren i Privacy Shield.

Det här innebär att i det fall Årjängs kommun avser överföra personuppgifter utanför EU/EES ska alltid ett särskilt beslut fattas om detta. Beslutet fattas av den personuppgiftsansvarige. Ett beslut om överförande av personuppgifter utanför EU/EES får endast fattas om den personuppgiftsansvarige bedömer att tillräckliga garantier givits om att personuppgifterna kommer att hanteras på ett säkert sätt. Beslutet ska dokumenteras.