Beslutad av: Kommundirektör Britt-Marie Börjesson
Datum: 2022-04-08
Börjar gälla: 2022-04-11
Dokumentansvarig tjänsteperson: Kanslichef
Följs upp: En gång per mandatperiod eller oftare vid behov

Diarienummer:
Ks 2022/59
Kommunal författningssamling
Nr F 22:03

REGELDOKUMENT | **RUTIN**

GDPR-rutin för Tomelilla kommun

Tomelilla kommun

Tomelilla kommuns styrdokument

Regeldokument
Regeldokument är dokument som talar om hur kommunen ska arbeta. Regeldokument kan också vara lokala föreskrifter om olika bestämmelser som kan påverka kommuninvånare eller företag.
REGELEMENTEN RIKTLINJER RUTINER

Målinriktade dokument
Målinriktade dokument visar vad kommunen vill uppnå, strävar efter eller har som mål.
VISION PROGRAM OCH STRATEGIER PLANER HANDLINGSPLANER

Innehållsförteckning

Inledning

Den 25 maj 2018 trädde EU:s nya dataskyddsförordning, (GDPR), i kraft. Förordningen ersätter personuppgiftlagen (1998:2014), PuL, och det bakomliggande direktivet till PuL.

Syftet med den nya dataskyddförordningen är att den ska skydda enskildas grundläggande rättigheter och friheter och då särskilt rätten till skydd av personuppgifter. Ett ytterligare syfte är att säkerställa att det finns ett adekvat dataskydd för de system där personuppgifter behandlas. Förordningen har även till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifterna inom EU. Förordningens syfte är även att modernisera dataskyddsdirektivets regler från 1995 och att anpassa det till det digitaliserade samhället.

Vikten av att den personuppgiftsansvarige (dvs. varje nämnd) kan visa att förordningen följs är en väsentlig del av förordningen och utgör en av de grundläggande rättsliga principerna (principen om ansvarsskyldighet). Detta medför bland annat ett utökat krav på dokumentation av hur personuppgifter behandlas inom kommunen. Skulle kommunen ha brister i sin personuppgiftsbehandling eller på annat sätt inte uppfylla de krav som ställs i förordningen riskerar kommunen att åläggas sanktionsavgift eller skadeståndsansvar.

Vad är personuppgifter?

En personuppgift är all den information som direkt eller indirekt kan identifiera en fysisk levande person. Exempel härpå är personnummer, personnamn, kontaktuppgifter, bilder, beskrivande eller värderande omdömen, identifikationsnummer eller IP-adress.

Förordningen omfattar all behandling av personuppgifter som sker helt eller delvis digitalt samt analog behandling, ”på papper”, om personuppgifterna ingår eller kommer att ingå i ett register. Definitionen på ”behandling” är alla tänkbara åtgärder man kan vidta med en personuppgift, såsom insamling, registrering, organisering, lagring, ändring, läsning, överföring, spridning, radering, bearbetning eller förstöring.

Syfte och omfattning

Det är viktigt för kommunen att personer känner sig trygga i hur vi behandlar deras personuppgifter och att vi upprätthåller en hög säkerhet för skyddet av deras uppgifter.

Grunden för all personuppgiftsbehandling är att det ska finnas ett specifikt, tydligt och berättigat ändamål med behandlingen och minst en laglig grund, samt att de grundläggande principerna ska beaktas.

Dessa principer innebär att alla personuppgifter alltid ska behandlas på ett lagligt, korrekt och öppet sätt gentemot den registrerade, och att personuppgifterna ska vara riktiga och uppdaterade, dvs. rätt uppgifter. Det är viktigt att tänka på att man inte behandlar fler personuppgifter än vad som är nödvändigt för att uppfylla ändamålet med behandlingen (principen om uppgiftsminimering) och att man inte behandlar personuppgifter för annat än det specifika ändamål man samlat in dem för (principen om ändamålsbegränsning). Därtill ska man gallra uppgifterna när ändamålet inte längre är aktuellt (lagringsminimering).

Undantagen till principerna om ändamålsbegränsning och lagringsminimering är då personuppgiftsbehandlingen sker för arkivändamål av allmänt intresse (allmänna handlingar), och för historiska, vetenskapliga, forsknings- eller statistikändamål.

Man ska även se till att endast de personer som måste ha tillgång till personuppgiften för sin yrkesutövning också bara är de som faktiskt behandlar personuppgiften i fråga. Personuppgiftsbehandlingen ska utföras på ett säkert sätt, avseende lämpligt tekniskt och organisatoriskt skydd mot obehörig åtkomst, intrång, förlust och förvanskning (principerna om integritet och konfidentialitet). En tumregel är att ju känsligare personuppgift desto starkare skydd krävs.

Inom Tomelilla kommun behandlas personuppgifter av olika slag och för skilda ändamål inom en rad olika verksamheter. Därav finns behovet av en kommunövergripande rutin för att sätta de ramar verksamheten behöver iaktta vid behandlingen av personuppgifter. Rutinen ska i sin tur kompletteras av ytterligare rutiner som på ett mer detaljerat sätt stödjer de olika verksamheterna i personuppgiftsbehandlingsfrågor och processer som uppstår.

Vem är ansvarig?

I Tomelilla kommun är varje nämnd och styrelse personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom respektive verksamhetsområde. Kommunen behöver behandla den registrerades personuppgifter för att kunna tillhandahålla den service och det stöd den ansvarar för. Det kan handla om personuppgifter för exempelvis elever, uppdragstagare, vårdtagare eller andra som har kontakt med kommunens verksamheter.

Rättsliga grunder

De vanligaste förekommande rättsliga grunderna inom de kommunala verksamhetsområdena är:

- Avtal (anställningsavtal, avtal om sophämtning etc.)

- Rättslig förpliktelse (ska vara fastställt i lag, kollektivavtal eller beslut)
- Allmänt intresse eller led i myndighetsutövning (allt från kärnverksamhet som äldreomsorg och bygglovshantering till frivilliga verksamheter som kulturskola och chattar med medborgare)
- Samtycke (bör tillämpas restriktivt och endast när ingen annan rättslig grund är tillämpbar, eftersom samtycke alltid kan återkallas)

Offentlighetsprincipen

Offentlighetsprincipen gäller fortfarande, men det är viktigt att vid en begäran om utlämnande av allmän handling, efter sedvanlig sekretessprövning, också pröva att utlämnandet inte strider mot GDPR. Enligt offentlighets- och sekretesslagen (OSL 2009:400) gäller sekretess för personuppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med förordningen. Detta får då anses utgöra ett undantag till efterforskningsförbudet.

Huvudregeln är alltså att offentlighet råder, men vid befogad misstanke, ”om man kan anta”, att frågeställaren ska komma att använda personuppgifterna i strid med GDPR får man ställa vissa kompletterande frågor. Om svaret känns trovärdigt ska uppgiften lämnas ut, annars inte. Exempel på när detta kan bli aktuellt är vid så kallat massuttag, dvs. om någon begär ut en stor mängd uppgifter antingen om en mängd olika personer eller en enskild individ.

Efterforskningen får endast sträcka sig till vad som är nödvändigt för att kunna pröva om sekretess ska föreligga.

Personuppgiftsbehandling

Varje behandling av personuppgifter ska ske med iakttagande av den enskildes integritet och med beaktande av de rättigheter som tillkommer de registrerade. Mot bakgrund av detta ska nedanstående följas:

- Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning.
- Behandlingen ska vara laglig, korrekt och öppen gentemot de registrerade.
- Innan behandling påbörjas ska ett särskilt och uttryckligt ändamål med behandlingen vara fastställt. Behandling av personuppgifter får inte ske för ett ändamål som är oförenligt med det ursprungliga ändamålet, med undantag för bland annat arkivändamål av allmänt intresse.
- Insamling av personuppgifter ska inte vara mer omfattande än nödvändigt. Detta innebär att endast uppgifter som är adekvata och relevanta får samlas in.
- Uppgifterna ska vara uppdaterade och korrekta.
- Insamlade personuppgifter ska endast bevaras i identifierbar form så länge det är nödvändigt för ändamålet och inte annat följer av lag.
- Åtkomst till personuppgifter ska begränsas till de som är behöriga.
- Organisatoriska och tekniska åtgärder för att skydda personuppgifterna ska vidtas i enlighet med utförda riskanalyser och säkerhetsklassningar.
- Personuppgiftsansvarig ska kunna påvisa sin följsamhet till dataskyddsförordningen och däri angivna regler/principer.
- Dataskyddsombud ska finnas utsett för kommunens samtliga nämnder.
- Varje behandling av personuppgifter ska ske på sådant sätt att risken för de registrerade minimeras.

Dataskyddsombud

I den europeiska dataskyddsförordningen fastslås att myndigheter måste utse ett dataskyddsombud. Detta ombud ska fungera som ett stöd för verksamheterna för att säkerställa att all behandling sker på ett korrekt sätt och att vi som kommun skyddar de uppgifter vi behandlar på ett lämpligt sätt. Tomelilla kommun har tillsammans med Ystads, Sjöbos och Simrishamns kommuner Annika Linderoth som dataskyddsombud. Hon kan nås på dataskyddsombudet@simrishamn.se.

Rättigheter enligt allmänna dataskyddsförordningen

Av förordningen följer ett antal rättigheter för de personer vars personuppgifter behandlas av kommunen.

- Rätt att få information om och tillgång till sina personuppgifter (registerutdrag).
- Rätt att begära rättelse eller komplettering av felaktiga uppgifter.
- Rätt att begära att personuppgifter raderas. (I praktiken en starkt kringskuren rättighet inom offentlig verksamhet på grund av offentlighetsprincipen och arkivlagen. Exempel på när det ändå kan förekomma är vid återkallat samtycke eller om personuppgifterna har behandlats i strid med lag.*)*
- Rätt att begära begränsning av kommunens behandling av personuppgifter. (Exempel härpå kan vara att den registrerade bestrider personuppgifternas korrekthet under tiden som kommunen granskar om de är korrekta, eller att personuppgifterna inte längre behövs.)

Om en registrerad vill begära ett registerutdrag för sig själv eller för sitt barn så kan hen vända sig till respektive nämnd där det finns en kontaktperson.

Vad gäller om personen samtyckt till att vi hanterar dess uppgifter?

Om personen i frågan har samtyckt till att kommunen hanterar hens personuppgifter har den registrerade alltid rätt att ångra sig och ta tillbaka sitt samtycke. Det gör hen genom att kontakta kommunen. Vid återkallat samtycke får kommunen inte längre behandla individens uppgifter. Om hen återkallar sitt samtycke påverkar det inte lagligheten av publiceringen innan samtycket återkallades.

Vad anses som känslig personuppgift?

Inom kommunal verksamhet är det vanligt förekommande att så kallade känsliga personuppgifter (enligt artikel 9) behandlas. Det ställs då högre krav för att få behandla dessa uppgifter (artikel 9.2). Dessa kan exempelvis vara följande:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa
- En persons sexualliv eller sexuella läggning
- Genetiska uppgifter
- Biometriska uppgifter som entydigt identifierar en person

Till vilka andra överlämnar vi personuppgifter?

Personuppgifter kan komma att lämnas ut till andra myndigheter, företag eller enskilda om kommunen har en laglig skyldighet att lämna ut dem. De kan

också lämnas till personuppgiftsbiträden som hanterar information för vår räkning. Vi har personuppgiftsbiträden som exempelvis hjälper oss med:

- Betalningar (fakturahantering, banker och betaltjänstleverantörer).
- Marknadsföring och information (reklambyråer, mediebyråer, utskrift och sociala medier).
- IT-tjänster (tillhandahålla verksamhetsstöd, hantera drift, support och underhåll av våra IT-lösningar).
- Personal (rekryteringsföretag, ledar- och medarbetarundersökningar, företagshälsovård).

Överföring till tredje land

Överföring till tredje land betyder att uppgifter lämnas till länder utanför EU och EES-länderna Norge, Island och Liechtenstein. Om vi som kommun överför personuppgifter till tredje land ska den berörda registrerade informeras om detta.

Personuppgiftsincidenter

Enligt en särskild definition i dataskyddsförordningen definieras begreppet personuppgiftsincident som en säkerhetsincident som leder till oavsiktlig eller annan olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller annan obehörig åtkomst till de behandlade personuppgifterna.

För att en incident ska utgöra en personuppgiftsincident som ska anmälas till Integritetsskyddsmyndigheten (IMY) ska den ha medfört en risk för den vars personuppgifter det handlar om. Riskerna kan utgöras av exempelvis identitetsstöld, bedrägeri, finansiell förlust, diskriminering eller skadlig ryktesspridning. Om det inte är osannolikt att personuppgiftsincidenten

medför en risk för fysiska personers rättigheter och friheter ska den anmälas till integritetsskyddsmyndigheten inom 72 timmar från att den upptäckts.

Hur vi behandlar incidenter?

En medarbetare som upptäcker en personuppgiftsincident ska omedelbart påbörja dokumentation av incidenten på blanketten ”Intern dokumentation av personuppgiftsincident” och anmäla detta till närmaste chef. Aktuell chef ska i sin tur omedelbart anmäla incidenten till verksamhetschef. Verksamhetschef ansvarar för att personuppgiftsansvarig meddelas.

Anmälan till IMY görs av den personuppgiftsansvarige, det vill säga ansvarig nämnd som bestämmer ändamål och medel för behandlingen. Varje nämnd har delegerat ansvaret till tjänsteman. Det finns också en skyldighet för den som har anlitats som personuppgiftsbiträde att uppmärksamma den personuppgiftsansvarige på en säkerhetsincident så fort den upptäckts.

Den personuppgiftsansvarige är under vissa omständigheter själv skyldig att informera de personer vars uppgifter berörs av incidenten. Den informationen ska bland annat omfatta vilka konsekvenser incidenten kan leda till och vilka åtgärder man vidtagit för att motverka eventuella negativa följder. Syftet är bland annat att göra det möjligt för de enskilda personerna att själva vidta nödvändiga åtgärder.

När Integritetsskyddsmyndigheten blir informerad om en incident kan myndigheten fatta beslut om att den personuppgiftsansvarige måste informera de registrerade eller att det inte är nödvändigt. Om de registrerade ska informeras kan Integritetsskyddsmyndigheten komma att ge råd om hur detta ska ske.

Frågor?

Har ni ytterligare frågor kontakta kommunsekreterare Thomas Lindberg via telefon 0417-182 93 eller mejl thomas.lindberg@tomelilla.se, eller dataskyddsombud Annika Linderoth, 0414-819 000 (växel) eller dataskyddsombudet@simrishamn.se.

Ytterligare information och blanketter finns på https://intranat.tomelilla.se/support/gdpr (intern) och extern information finns på https://www.tomelilla.se/kommun-och-politik/demokrati-och-insyn/gdpr.