STYRDOKUMENT

Riktlinjer för behandling av personuppgifter

Beslutad när	2019-05-16 § 109
Beslutad av	Kommunfullmäktige
Diarienummer	KSKF/2018:47
Ersätter	Instruktion enligt personuppgiftslagen (1998:204) för Eskilstuna kommunkoncern Antagen av kommunfullmäktige den 23 september 2010, § 193
Gäller för	Samtliga nämnder
Gäller fr o m	2019-05-16
Gäller t o m	Tillsvidare
Dokumentansvarig	Administrativa direktören Lena Lundberg
Uppföljning	Löpande

Program
Ett program är ett styrande dokument som ska visa en färdriktning genom att innehålla vad som ska uppnås inom ett visst område. Det tar inte ställning till utförande, prioriteringar och metoder. Program ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Plan
En plan är ett styrande dokument som ska visa en färdriktning genom att innehålla konkreta mål och riktlinjer. Den ska vara tidsbegränsad och beslutas av kommunfullmäktige.

Policy
En policy är ett styrande dokument som ska visa ett övergripande förhållningssätt och som ska tjäna som vägledning inom ett område, med angivande av övergripande mål och värden som ska eftersträvas. Policys ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Riktlinje
En riktlinje är ett styrande dokument som ska säkerställa ett korrekt agerande och god kvalitet i handläggning och utförande. Riktlinjer ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Ämnesområde och bakgrund

Behandlingar av personuppgifter regleras i 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 (Dataskyddsförordningen).

Syftet med dataskyddsförordningen är dels att man vill stärka privatpersoners rättigheter genom att förenkla och ge dem bättre kontroll över sina personuppgifter och dels att anpassa regelverket till den tekniska utvecklingen, med internet, sökmotorer, sociala medier mm.

Inledning

Dataskyddsförordningen gäller för helt eller delvis automatiserad behandling av personuppgifter. Den gäller också för manuell behandling av personuppgifter om personuppgifterna ingår i eller är avsedda att ingå i ett manuellt register som är sökbart enligt särskilda kriterier.

Personuppgifter är alla uppgifter som direkt eller indirekt kan knytas till en fysisk person. De vanligaste typerna av personuppgifter som förekommer i en kommuns olika system är antingen *direkta personuppgifter* eller *indirekta personuppgifter*. Exempel på direkta personuppgifter är namn, foto, födelsedatum, personnummer och på indirekta personuppgifter är fastighetsbeteckning, adress, IP-nummer, ärendenummer och användar-ID.

Med begreppet behandling av personuppgifter avses alla former av åtgärder, till exempel insamling, registrering, användning och lagring. Dataskyddsförordningen gäller oavsett på vilket sätt uppgifterna lagras. Det kan t.ex. vara i en dator, på sociala medier, i e-postlådor eller på webbsidor. Personuppgifter ska så långt det är möjligt lagras i behörighetsstyrda system.

I en kommun är varje nämnd en myndighet och personuppgiftsansvarig för att all behandling av personuppgifter inom nämndens verksamhetsområde.

För att överhuvudtaget få behandla personuppgifter krävs att den personuppgiftsansvarige kan åberopa en *rättslig grund* (se vidare nedan).

Den personuppgiftsansvarige ska tydligt beskriva varför personuppgifterna samlas in genom att ange *ändamålet* för behandlingen. Det innebär att ändamålet ska vara väl beskrivet, tydligt avgränsat, dokumenterat och kommunicerat. Personuppgifterna får därefter inte användas för ett annat ändamål.

Den personuppgiftsansvarige ska sträva efter att minimera antalet personuppgifter som behandlas och lagras. Inaktuella personuppgifter ska raderas och gallras permanent från alla lagringsutrymmen, i enlighet med

varje nämnds dokumenthanteringsplan. Dataskyddsförordningen hindrar inte att personuppgifter bevaras för arkivändamål, även om de ursprungligen samlades in för ett annat ändamål.

Behandling av personuppgifter ska det göras på ett korrekt och öppet sätt i förhållande till den registrerade.

Förordningen innebär i huvudsak att Eskilstuna kommun ska

- Fördela ansvaret mellan kommunstyrelsen och nämnderna.
- Kartlägga vilka personuppgifter vi behandlar och varför.
- Analysera riskerna för att en persons integritet, rättighet och frihet kränks samt bedöma vilken skada som kan uppstå.
- Bygga in ett standardiserat dataskydd i system och processer.
- Dokumentera behandlingen så att vi kan bevisa att vi uppfyller kraven.
- Kunna informera de registrerade, allmänheten och medarbetare om hur personuppgifter behandlas och om vem som har ansvaret.
- Skapa rutiner för samtycken.
- Skapa rutiner för hur vi ska hantera incidenter, problem och klagomål.

Ansvarsfördelning

För att leva upp till dataskyddsförordningens krav, är det viktigt att alla förtroendevalda, chefer och medarbetare behandlar personuppgifter i enlighet med dataskyddsförordningens krav.

Kommunstyrelsen och Servicenämnden

Kommunstyrelsen är ansvarig för framtagande och uppföljning av kommunövergripande styrdokument.

Kommunledningskontoret ska leda arbetet med framtagandet av ett inbyggt dataskydd för personuppgifter som en del av informationssäkerhetsarbetet.

Servicenämnden ska erbjuda tjänsten som dataskyddsombud .

Serviceförvaltningen ska även erbjuda tjänsten som dataskyddskoordinator med uppgift att stödja och utveckla verksamheten utifrån de personuppgiftsansvarigas behov (se vidare nedan).

Dataskyddsombuden och dataskyddskoordinatorn ska årligen informera kommunstyrelsen om hur arbetet fortlöper och hur förordningen efterlevs.

Personuppgiftsansvarig nämnd

Varje nämnd är en myndighet och ansvarig för att all behandling av personuppgifter inom nämndens verksamhetsområde behandlas i enlighet

dataskyddsförordningens föreskrifter, oavsett arbetsplats, verktyg och arbetstid.

Varje nämnd ska utse ett dataskyddsombud och en dataskyddssamordnare.

Varje nämnd ska ta fram en handlingsplan för hur de ska arbeta med personuppgifter inom sin nämnd.

Dataskyddssamordnarna ska i huvudsak ha följande ansvar.

- Stödja nämnden i implementeringen av förordningen.
- Föreslå förvaltningsspecifika rutiner.
- Upprätta och vårda nämndens registerförteckning.
- Följa upp nämndens handlingsplan.
- Följa upp beslutade åtgärdsplaner.
- Samordna nämndens information vid begäran om utlämnande av registerutdrag.

Varje nämnd är ansvarig för att samtliga chefer och medarbetare får information om och tillägnar sig de kunskaper som krävs samt får det stöd de behöver för att leva upp till dataskyddsförordningens regelverk.

Enligt dataskyddsförordningen finns det sanktioner vid felbehandling av personuppgifter.

Varje nämnd ansvarar för de straff- och skadeståndsanktioner som kan uppkomma på grund av felaktig behandling av personuppgifter. Vid nämndövergripande personuppgiftsbehandlingar ska de nämnder som behandlar personuppgifterna gemensamt komma överens om hur ansvaret och eventuella sanktionsavgifter ska fördelas. En sådan överenskommelse ska diarieföras.

Systemägare och systemförvaltare
Alla system som behandlar personuppgifter ska ha en systemägare och minst en systemförvaltare. Vilka de är ska framgå av nedan angivna registerförteckning.

Kommunstyrelsen eller servicenämnden ska vara systemägare för kommunövergripande system.

Systemägaren ska tillsammans med systemförvaltaren skriva en systemförvaltningsplan, där de utifrån det beskrivna ändamålet ska precisera hur de ska uppnå en uppgiftsminimering och lagringsminimering, samt i de fall det görs en konsekvensbedömning (se nedan), vilket dataskydd som krävs.

Systemförvaltaren ska förvalta systemet och kontinuerligt informera systemägaren om händelser och behandlingar som kan påverka den registrerades rättigheter på ett negativt sätt.

Personuppgiftsbiträde
Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för en personuppgiftsansvarigs räkning.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställa att den registrerades rättigheter skyddas.

De personuppgiftsansvariga ska teckna ett skriftligt personuppgiftsbiträdesavtal med personuppgiftsbiträdet. Av avtalet ska framgå hur personuppgiftsbiträdet ska hantera eventuella personuppgifter.

Chefer och medarbetare

Alla chefer och medarbetare är skyldiga att tillägna sig de kunskaper som krävs för att kunna sköta sina arbetsuppgifter. Detta innebär framförallt att alla medarbetare och chefer ska kunna urskilja vad som är en personuppgift och säkerställa att uppgifterna behandlas enligt dataskyddsförordningen.

Dataskyddsombud

Ett dataskyddsombud är en tvingande funktion som ska

- Kontrollera att nämnderna följer dataskyddsförordningen och beslutade styrdokument.
- Samla in information om hur den personuppgiftsansvarige behandlar personuppgifter, sammanställa informationen och informera om det finns behandlingar som behöver åtgärdas.
- Informera och ge råd till chefer och medarbetare inom organisationen, så att de kan göra rätt vid behandling av personuppgifter.
- På begäran från en nämnd ge råd och bistå vid konsekvensbedömningar.
- Vara kontaktperson och samarbeta med Datainspektionen.
- Vara kontaktperson för de registrerade.

Dataskyddskoordinator

Serviceförvaltningen ska erbjuda tjänsten som dataskyddskoordinator för att kunna göra följande.

- Ge råd och stöd i personuppgiftsfrågor.
- Ansvara för framtagande av rutiner.
- Utbilda medarbetare.
- Göra sekretessbedömningar vid utlämnande av registerutdrag.
- Ge råd och stöd vid tecknandet av personuppgiftsbiträdesavtal.

Dataskyddskoordinatorn ska även tillsammans med dataskyddsamordnarna ta fram förslag på kommungemensamma åtgärder för att bl a

- Underlätta upptäckten av personuppgiftsincidenter.
- Kunna hantera en faktisk personuppgiftsincident.
- Kunna dokumentera alla personuppgiftsincidenter, även de som inte måste anmälas till Datainspektionen.

Rättslig grund för behandlingen

För att få behandla personuppgifter krävs att kommunen kan hänvisa till en rättslig grund. Dessa är följande.

- Samtycke från den registrerade.
- För att fullgöra ett avtal.
- För att fullgöra en rättslig förpliktelse.
- För att skydda registrerades intresse.
- För att fullgöra ett allmänt intresse.

Alla personuppgiftsbehandlingar som utförs omfattas av dataskyddsförordningen.

För de fall en personuppgiftsbehandling även berör andra lagar och förordningar måste en bedömning om vilka regler som har företräde göras i varje enskilt fall.

Registerförteckning

Enligt dataskyddsförordningen ska den som är personuppgiftsansvarig upprätta en registerförteckning som visar vilka personuppgiftsbehandlingar som hanteras.

Även personuppgifter som hanteras på ett ostrukturerat sätt, såsom i epost eller lagras i hemkataloger, ska framgå av registerförteckningen.

Varje nämnd ska ha en samlad registerförteckning över sina behandlingar.

Förteckningen ska innehålla i huvudsak följande uppgifter.

- Namn och kontaktuppgifter för den personuppgiftsansvarige.
- Utsett dataskyddsombud.
- Rättslig grund för behandlingen.
- Ändamålet med behandlingen.
- Tekniska och organisatoriska säkerhetsåtgärder.
- Kategorier av registrerade personer.
- Typer av personuppgifter.
- Tidsfrister för radering.

Behandling av känsliga personuppgifter är förbjuden, om det inte går att åberopa något av de i dataskyddsförordningen angivna undantagen.

Känsliga personuppgifter är följande.

- Etniskt ursprung
- Politisk uppfattning
- Religiös eller filosofisk övertygelse
- Fackligt medlemskap
- Sexualitet och hälsa

Skyddad identitet ska betraktas som en känslig personuppgift och uppgifterna ska ha extra skyddsåtgärder.

Vissa skyddsåtgärder är dessutom extra skyddsvärda.

Extra skyddsvärda personuppgifter är

- Personuppgifter som tillhör barn under 16 år
- De fyra sista siffrorna i personnumret
- Viss ekonomisk information
- Uppgifter som innehåller sekretess

Extra skyddsvärda uppgifter som kommuniceras via öppna nätverk ska minst vara skyddad genom stark autentisering, enligt rådande godkänd standard.

Personuppgifter som kräver extra skyddsåtgärder och ska överlämnas till annan via internpost ska levereras i ett säkerhetskuvert.

Registerförteckningen ska uppdateras löpande och diarieföras i kommunens dokument- och ärendehanteringssystem.

Personuppgifter som är gemensamma för två eller fler nämnder ska förtecknas i varje enskild nämnds registerförteckning och diarieföras för varje enskild nämnd. Av registerförteckning ska det framgå att behandlingen avser flera personuppgiftsansvariga.

Konsekvensbedömning

Enligt dataskyddsförordningen ska den personuppgiftsansvarige inför behandlingar som kan utgöra en särskild stor risk, göra en konsekvensbedömning för att kunna avgöra om behandlingen är proportionell i förhållande till de risker som den kan medföra för den registrerade och vilken eventuell skada de kan orsaka.

Konsekvensbedömningar ska exempelvis göras vid

- Upphandling och inköp av system, program, tjänster och/applikationer.
- Användning av ny teknik.
- Många användare kan komma åt personuppgifterna.
- Behandlingen avser många personer.

- Behandlingen avser en stor mängd personuppgifter.
- Personuppgifter hanteras, kommuniceras och/eller lagras via öppna nätverk som internet.
- Personuppgifterna hanteras/lagras av en extern leverantör.

Finner den personuppgiftsansvarige att personuppgifter behöver skyddas ska lämpliga tekniska och organisatoriska åtgärder tas fram som beskriver den säkerhetsnivå som är lämplig i förhållande till tillgänglig teknik och kostnaden för åtgärderna.

Till tekniska åtgärder räknas till exempel brandväggar, krypteringsfunktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, rutiner och instruktioner. Åtgärderna ska föras in i registerförteckningen.

Konsekvensbedömningen ska diarieföras tillsammans med registerförteckningen.

Inbyggt dataskydd och dataskydd som standard

Det är den personuppgiftsansvarige som utifrån den ovan nämnda konsekvensbedömningen har ansvaret för att bestämma vilket dataskydd som krävs.

Kommunen ska sträva efter att skapa ett inbyggt dataskydd i alla system och ha dataskydd som standard, så att systemen, tjänsterna och rutinerna kan uppfylla de personuppgiftsansvarigas säkerhetskrav.

Detta kan uppnås genom i huvudsak följande åtgärder.

- Minimera mängden personuppgifter i systemen.
- Begränsa åtkomsten till uppgifterna genom behörighetsstyrning.
- Säkra autentiseringar genom flerfaktorsinloggningar.
- Skapa krypteringsfunktioner.
- Skapa säkrare fysiska enheter (t.ex. telefoner, datorer, servrar).
- Genomföra utbildningar.
- Skapa pseudonymisering.

Dokumentation, gallring och arkivering

De personuppgiftsansvariga ska registrera följande dokument i kommunens dokument- och ärendehanteringsystem.

- Registerförteckning över personuppgiftsbehandlingar
- Eventuella handlingsplaner
- Eventuella åtgärdsplaner
- Utsedda dataskyddsombud
- Förteckning över personuppgiftsbiträdesavtal
- Förteckning över inhämtade samtycken

- Genomförda konsekvensbedömningar
- Begäran om utlämnande av registerutdrag jämte svaret till frågeställaren
- Incidentrapporteringar

Nämndernas dokumenthanteringsplaner ska reglera vad som gäller för gallring och arkivering.

Information till den registrerade

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter.

Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige, både när uppgifterna samlas in och när den registrerade annars begär det.

Vid personuppgiftsinhämtning ska följande information framgå.

- Rättslig grund
- Syftet med personuppgiftsinsamlingen
- Hur det kommer att behandlas och lagras
- Den registrerades rättigheter
- Information om samtycke och återkallning av detsamma

Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar en personuppgiftsincident i vilken personuppgifter har raderats eller manipulerats.

För att en medborgare ska kunna begära ut personuppgifter som lagrats om denne måste denne legitimera sig. Vederbörande har bara rätt att begära ut uppgifter på sig själv.

Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för fysiska personers rättigheter och friheter, såsom exempelvis brott mot sekretess eller tystnadsplikt, finansiell förlust, diskriminering, identitetsstöld, bedrägeri eller skadlig ryktesspridning

En personuppgiftsincident har exempelvis inträffat om uppgifter som avser en eller flera registrerade personer har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer, oavsett om det skett oavsiktligt eller med avsikt.

Den personuppgiftsanvarige ska utan dröjsmål anmäla incidenten till dataskyddsombudet. Dataskyddsombuden ska delta i hela processen för att hantera och anmäla en incident. Dataskyddsombudet ska därefter inom 72 timmar från att incidenten upptäckts anmäla incidenten till Datainspektionen.

Behandlas personuppgifter av ett personuppgiftsbiträde ska de omedelbart rapportera incidenten till den personuppgiftsansvarige, som ytterst har det juridiska ansvaret.

Gällande lagstiftning

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 (GDPR).

Förhållande till andra styrdokument

Informationssäkerhetsplan för Eskilstuna kommun; KSKF/2014:112