Eda kommun

Riktlinjer för hantering av personuppgifter enligt dataskyddslagstiftningen (GDPR)

– Styrdokument –

Eda kommun	Styrdokument	
	Dokumenttyp	Riktlinje
	Beslutad av	Kommunstyrelsen 2018-05-17, § 119
	Dokumentansvarig	Kommunchefen
	Reviderad av	–

Innehållsförteckning

Inledning

EU:s dataskyddsförordning (General Data Protection Regulation; GDPR) har som syfte att skapa enhetliga dataskyddsregler i hela Europa, och skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av personuppgifter. Förordningen innehåller bestämmelser om när personuppgifter får samlas in, hur de får behandlas, hur de registrerade ska informeras m.m.

Dataskyddslagen är den nationella lagstiftning som kompletterar förordningen, och anpassar den till svenska förhållanden.

EU:s dataskyddsförordning och Dataskyddslagen är subsidiära i förhållande till annan lag eller förordning, och ska inte tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Grundläggande definitioner

Personuppgift

Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, t.ex. personnummer, namn, adress, fastighetsbeteckning, bild- och ljudupptagningar. Bedömning om det är fråga om en personuppgift behöver alltid göras i det enskilda fallet. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

Behandling av personuppgift

Med behandling avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter. Det kan vara t.ex. insamling, registrering, lagring, bearbetning eller sammanställning.

Personuppgiftsansvarig

Personuppgiftsansvarig är en fysisk eller juridisk person eller myndighet som bestämmer ändamålen med och medlen för behandling av personuppgifter.

Personuppgiftsansvarige har det yttersta ansvaret för att lagstiftning följs och den registrerades uppgifter behandlas korrekt. Den faktiska behandlingen av personuppgifter kan överlåtas till annan part, men personuppgiftsansvaret kan aldrig överlåtas.

Personuppgiftsbiträde

Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person som *externt* hanterar personuppgifter för den personuppgiftsansvariges räkning, t.ex. lönesystem eller ekonomisystem.

Personuppgiftsansvarig ansvarar för att det finns ett skriftligt avtal (personuppgiftsbiträdesavtal) med personuppgiftsbiträdet, som anger att biträdet enbart får behandla uppgifter i enlighet med personuppgiftsansvariges instruktioner.

Personuppgiftsincident

En säkerhetsincident som leder till oavsiktlig eller 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 obehörig åtkomst till de behandlade personuppgifterna.

Dataskyddsombud

Av personuppgiftsansvarig utsedd person som självständigt ser till att den personuppgiftsansvarige behandlar personuppgifter på ett korrekt och lagligt sätt. Dataskyddsombudet har en tillsynsuppgift.

Grundläggande principer för behandling av personuppgifter

All behandling av personuppgifter måste uppfylla ett antal grundläggande principer, som ska iakttas vid all behandling.

Laglighet, korrekthet och öppenhet

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Detta innebär att det måste finnas en rättslig grund för behandlingen, samt att det ska framgå klart och tydligt för den registrerade hur hans eller hennes personuppgifter samlas in och i övrigt behandlas.

Ändamålsbegränsning

Personuppgifter får bara samlas in för särskilda, uttryckligen angivna och berättigade ändamål. Ändamålet med behandlingen ska vara klargjort innan uppgifterna samlas in, och får inte vara alltför opreciserat eller omfattande.

Personuppgifter får efter insamling inte behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet. Dock får insamlade personuppgifter behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen, om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är förenliga med de ursprungliga ändamålen, ska de registrerade informeras om detta.

Uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är inte tillåtet att samla in personuppgifter för obestämda framtida behov. Insamlade personuppgifter får inte heller behandlas om de t.ex. är så gamla att de inte längre är relevanta för de ursprungliga ändamålen.

Korrekthet

Insamlade personuppgifter ska vara korrekta och uppdaterade. Alla rimliga åtgärder ska vidtas för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål. Om det krävs för ändamålen ska personuppgifterna vara uppdaterade.

Lagringsminimering

Personuppgifter får inte sparas, det vill säga förvaras i en form som möjliggör identifiering av den registrerade, under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När personuppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras.

Insamlade personuppgifter får lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Integritet och konfidentialitet

Personuppgifter ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse.

Ansvarsskyldighet

Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs, och ska kunna visa på vilket sätt dessa efterlevs.

Tillåten behandling av personuppgifter

Dataskyddsförordningen ger i huvudsak den registrerade bestämmanderätt över sina egna personuppgifter, dvs. behandling får bara ske om den registrerade lämnat samtycke till detta. Kommunala myndigheters behandling av personuppgifter får dock ske även om samtycke inte lämnats, om behandlingen är nödvändig för vissa angivna ändamål (se 4.1.1 – 4.1.3).

För att behandling av personuppgifter ska få ske inom kommunal verksamhet behöver, utöver de grundläggande principerna, även någon av följande rättsliga grunder vara uppfyllda.

Avtal och rättslig skyldighet

Behandling av personuppgifter får ske om det krävs för att ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas. Med detta avses t.ex. ansökan om barnomsorg, platsansökan, kö till hyreslägenheter m.m. Det måste vara den registrerade själv som är avtalspart. Om kommunen har träffat ett avtal med en juridisk person medför inte bestämmelsen rätt att behandla personuppgifter om t.ex. anställda hos den juridiska personen.

Den personuppgiftsansvarige får även behandla personuppgifter om det krävs för att fullgöra en rättslig skyldighet som kommunen har. Det kan exempelvis handla om förteckningar som miljöförvaltningen behöver för att utföra tillsyn enligt miljöbalken och livsmedelslagen eller om registrering av skolpliktiga barn.

Vitala intressen och allmänt intresse

Personuppgifter får behandlas om det är nödvändigt för att skydda vitala intressen som är av livsviktig och grundläggande betydelse för den registrerade. Exempelvis kan det i vissa fall vara nödvändigt att behandla personuppgifter för en person som är medvetslös och behöver vård.

Personuppgifter får också behandlas om det är nödvändigt för att en arbetsuppgift av allmänt intresse ska kunna utföras, såsom t.ex. arkivering, forskning, framställning av statistik m.m.

I samband med myndighetsutövning

Personuppgifter får behandlas om det är nödvändigt för att den personuppgiftsansvarige eller en tredje part till vilken personuppgifter lämnas ut ska kunna utföra en arbetsuppgift i samband med myndighetsutövning. Det behöver alltså inte vara en behandling i myndighetsutövning utan det räcker med att behandlingen sker i samband med myndighetsutövningen för att den ska vara tillåten.

Samtycke

Behandling, utöver ovanstående ändamål, är tillåten om den registrerade samtycker till behandlingen. Samtycke ska inhämtas innan behandling påbörjas, och lämnas genom ett uttalande eller en entydig bekräftande handling. Inhämtas samtycke i samband med en ansökan som den registrerade gör, ska det tydligt framgå för sökanden att denne även lämnar ett samtycke.

Den registrerade ska få tillräcklig information om behandlingen för att förstå innebörden av samtycket. Det är också viktigt att samtycket är frivilligt, och det kan vara tidsbegränsat.

Dataskyddslagen föreslår att ett barn som är minst 13 år ska kunna samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster, t.ex. sociala medier. En anhörig kan inte lämna samtycke för exempelvis en dement person, men samtycke kan lämnas av en förvaltare och i vissa fall av en god man.

Intresseavvägning

Om behandling av personuppgifter inte annars är tillåten, kan den personuppgiftsansvarige göra en intresseavvägning. Om kommunens intresse kan anses väga tyngre än den registrerades intresse av skydd mot kränkning får behandling ske. Intresseavvägningen kan även motivera behandling av personuppgifter om andra än avtalsparten, såsom anhöriga eller kontaktpersoner. Det kan t.ex. gälla registrering av närmast anhöriga till anställda. Dock bör behandlingen upphöra om den registrerade begär det.

När behandling av personuppgifter inte är tillåten

Samtycke återkallas

Ett lämnat samtycke till behandling av personuppgifter kan återkallas.

Ett återkallande av samtycke påverkar inte lagligheten av behandling som ägde rum före återkallandet, om behandlingen skedde i enlighet med förordningen. All fortsatt behandling ska vid ett återkallande dock upphöra, och ytterligare personuppgifter om den registrerade får inte behandlas. Detta förutsatt att det inte finns en rättslig grund för fortsatt behandling.

Rätt till radering (”rätten att bli bortglömd”)

Den registrerade har, med vissa undantag, rätt att utan dröjsmål få sina personuppgifter raderade. Undantag gäller om behandlingen är nödvändig för att:

- utöva rätten till yttrande- och informationsfrihet,
- uppfylla en rättslig förpliktelse,
- utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige,
- kunna fastställa, göra gällande eller försvara rättsliga anspråk,
- möjliggöra arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Känsliga personuppgifter

Behandling av känsliga personuppgifter är som huvudregel förbjudet. Känsliga personuppgifter är personuppgifter som

- avslöjar ras eller etniskt ursprung,
- avslöjar politiska åsikter,
- avslöjar religiös eller filosofisk övertygelse,
- avslöjar medlemskap i fackförening,
- behandlar genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person, eller
- rör hälsa eller sexualliv.

Undantag

Liksom för icke känsliga personuppgifter kan den registrerade lämna sitt samtycke. Den registrerades uttryckliga samtycke medför att behandling av känsliga personuppgifter blir tillåten.

Med samtycke jämställs att den registrerade på ett tydligt sätt offentliggjort uppgifterna. De förtroendevaldas partitillhörighet är en sådan uppgift.

Om samtycke saknas kan känsliga personuppgifter ändå behandlas om det är nödvändigt för att

- den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten,
- den registrerades vitala intressen ska kunna skyddas och den registrerade inte kan lämna sitt samtycke, eller
- rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras.

Uppgifter om personnummer eller samordningsnummer får utan samtycke enbart behandlas när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Födelsedatum räknas inte som personnummer och kan skrivas ut på förteckningar om personuppgiftsbehandlingen i övrigt är tillåten.

Information till den registrerade

Den registrerade har rätt att få tydlig information om vad en personuppgiftsbehandling avser.

Allmän information

På kommunens hemsida ska det finnas en allmän information om kommunens behandling av personuppgifter. Här presenteras hur personlig information samlas in och används, den registrerades rättigheter och hur dessa rättigheter görs gällande, samt kontaktuppgifter vid eventuella frågor.

Information inför personuppgiftsbehandling

Information om en specifik behandling av personuppgifter ska alltid ges till den registrerade *innan* behandlingen påbörjas. Inhämtas personuppgifterna från den registrerade själv, lämnas information lämpligast i samband med insamlandet. Inhämtas personuppgifterna från någon annan part, ska den personuppgiftsansvarige lämna information i samband med att personuppgifterna första gången registreras. Information behöver inte lämnas om det finns andra bestämmelser som gäller framför dataskyddsförordningen, t.ex. om vissa uppgifter omfattas av sekretess.

Informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, dvs. kommunens adress, nämnd och kontaktperson, uppgift om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgift och rätten att ansöka om information och få rättelse. Den registrerade ska om möjligt även få kännedom om hur länge personuppgifterna finns lagrade.

Undantag
Information behöver inte lämnas om sådant som den registrerade redan känner till, eller om det är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Information vid begäran om registerutdrag

Den registrerade har rätt att av den personuppgiftsansvarige få information om huruvida personuppgifter som rör honom eller henne håller på att behandlas, och i så fall få tillgång till personuppgifterna. Vid en begäran om registerutdrag ska personuppgiftsansvarige lämna följande information:

- vilka uppgifter om sökande som behandlas,
- varifrån dessa uppgifter har hämtats,
- ändamålen med behandlingen,
- till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut,
- eventuell överföring till tredje land, och i så fall vilka skyddsåtgärder som har vidtagits,
- hur länge verksamheten sparar uppgifterna, och
- förekomsten av automatiserat beslutsfattande och vilka följderna blir för den registrerade.

Personuppgiftsansvarige ska även informera den registrerade om rätten att lämna klagomål till Datainspektionen, rätten att bli raderad (om det inte står i strid med offentlighetsprincipen), samt rätten att invända mot och begära begränsning av en personuppgiftsbehandling.

Den sökande har rätt att få ett skriftligt besked inom en månad från att ansökan inkom. Om beskedet tar längre tid, ska den sökande underrättas om detta innan en månad har passerat.

Undantag
Om sekretess eller tystnadsplikt gäller mot den registrerade själv för vissa uppgifter ska sådana uppgifter inte lämnas i registerutdraget. Det kan exempelvis vara fråga om sekretess gentemot patient enligt 25 kap. 6 § offentlighets- och sekretesslagen.

Ansvar och organisation

Personuppgiftsansvarig

I en kommun är respektive nämnd och styrelse personuppgiftsansvarig. I Eda är kommunstyrelse, valnämnd, jävsnämnd, överförmyndarnämnd, kommunrevisorer samt respektive bolagsstyrelse personuppgiftsansvarig inom sitt verksamhetsområde.

Personuppgiftsansvarig har följande ansvar:

- upprätta förteckning över de behandlingar som personuppgiftsansvarig genomför,
- säkerställa och kunna visa att behandlingar utförs i enlighet med EU:s dataskyddsförordning och den nationella dataskyddslagen,
- ta fram lämpliga strategier för dataskydd,
- ta fram riktlinjer för hantering av behandlingsrelaterade händelser; så som registerutdrag, rätta felaktiga uppgifter och personuppgiftsincident,
- tydligt kommunicera hur hanteringen av dataskyddet samt den personliga integriteten hanteras i kommunen,
- skadeståndsansvar gentemot registrerad vid incident,
- utse dataskyddsombud

Dataskyddsombud

Eda köper tjänst som dataskyddsombud externt. Dataskyddsombudet ansvarar för att övervaka efterlevnaden av dataskyddsförordningen genom att:

- vara ett kunskapsstöd inom Eda kommun gällande dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- självständigt övervaka den interna efterlevnaden av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- rapportera till organisationens ledning om dataskyddsfrågor och organisationens brister och utvecklingsbehov minst en gång per år, samt ge förslag på åtgärder och utveckling.

- om den personuppgiftsansvarige inte inom rimlig tid rättar till påpekade brister har ombudet skyldighet att anmäla förhållandet till Datainspektionen
- tillsammans med sakkunniga inom Eda kommun kravställa och arbeta för att införa säkerhetsskyddsåtgärder enligt lagstiftning inom dataskydd
- bevaka och kravställa dataskydd vid upphandling av verksamhetssystem och dylikt
- identifiera kompetensutvecklingsbehov, planera och genomföra utbildningar avseende dataskyddsförordningen och angränsande lagstiftning
- övervaka den interna efterlevnaden av organisationens strategi för dataskydd
- ta fram konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär integritetsrisker, samt anmäla dessa till Datainspektionen för förhandskontroll
- bistå i utredning av misstänkta dataintrång
- informera Datainspektionen vid personuppgiftsincident inom 72 timmar
- omvärldsbevakning och nätverkande/kunskapsinhämtning rörande dataskyddslagen, dataskyddsförordningen och patientdatalagen
- fungera som kontaktpunkt för tillsynsmyndigheten, och vid behov genomföra förhandssamråd
- ta fram personuppgiftsbiträdesavtal och hjälpa till att granska de avtal som biträden skickar till den personuppgiftsansvarige
- erbjuda utbildning inom området dataskyddslagstiftning
- delta vid Dataskyddsgruppens planerade sammanträden
- bistå i framtagande/revidering av rutiner och riktlinjer kring dataskydd
- ta emot, koordinera, sammanställa och förmedla kommunens enhetliga svar på begäran om registerutdrag inom de stipulerade 30 dagarna, samt meddela den sökande i händelse av att svar tar längre tid än dessa 30 dagar
- hjälpa registrerade att erhålla rättelse eller radering

Dataskyddsgrupp

I organisationen kring dataskyddsombudet finns en dataskyddsgrupp bestående av representanter från avdelningar och verksamheter inom förvaltningen, samt representanter för de kommunala bolagen. Gruppen har till uppgift att:

- vara kontaktpersoner för dataskyddsombudet
- vara kontaktperson för respektive avdelning/verksamhet i dataskyddsfrågor

- koordinera respektive avdelnings/verksamhets dataskyddsarbete
- förteckna respektive avdelnings/verksamhets personuppgiftsbehandlingar i kommunens registerförteckning
- ta fram övergripande såväl som verksamhetsanpassade mallar, rutiner och processer för registrerades rättigheter
- se över samtyckesblanketter som respektive verksamhet använder så att den registrerade tydligt ser vad som registreras, för vilket syfte och hur länge informationen förväntas lagras
- sammanställa information om behandlingar från respektive verksamhet vid begäran om registerutdrag, och överlämna till dataskyddsombud inom stipulerad tid

Sammankallande för dataskyddsgruppen

Sammankallande har en har en sammanhållande roll för dataskyddsgruppen genom att:

- ansvara för att sammankalla och koordinera dataskyddsgruppen
- vara kontaktperson internt och externt genom att t.ex. svara på enklare frågor, ge allmän vägledning, förmedla kontakter och dirigera frågor till rätt funktion inom organisationen

Delegation

För övriga frågor vad gäller dataskyddsarbete framgår befattningshavare i kommunstyrelsens delegationsordning. Kommunstyrelsen delegerar t.ex. till kommunchef och verksamhetschefer att underteckna personuppgiftsbiträdesavtal.

Säkerhet vid behandling

Den personuppgiftsansvarige är skyldig att vidta lämpliga säkerhetsåtgärder för att skydda de personuppgifter som behandlas och förvaras inom verksamheten. Ett led i detta arbete är att kartlägga integritetsrisker och skapa rutiner för personuppiftsincidenter. Målet är att kontinuerligt förbättra kommunens informationssäkerhet.

Kartläggning av integritetsrisker

Dataskyddsombud ansvarar för att göra en konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär integritetsrisker, t.ex. kameraövervakning, genetiska register eller inom sjukvården.

Konsekvensbedömningar för känsliga behandlingar anmäls till Datainspektionen som gör en förhandskontroll och säkerställer att behandlingen är i enlighet med förordningens regler.

Åtgärder vid personuppgiftsincident

Vid en personuppgiftsincident ska dataskyddsombud, så snart som möjligt inom 72 timmar, anmäla incidenten till Datainspektionen. I somliga fall beslutar Dataskyddsinspektionen att personuppgiftsansvarig ska informera den registrerade om incidenten.

Dataskyddsombudet ansvarar för att tillsammans med dataskyddsgruppen utarbeta en rutin som ska gälla för hantering av personuppgiftsincident.

Rättsliga konsekvenser

Ansvaret för behandling av personuppgifter, som ytterst ligger på personuppgiftsansvarig, är straff- och skadeståndssanktionerat.

Varje person som lidit materiell eller immateriell skada till följd av överträdelser av EU:s dataskyddsförordning har rätt till ersättning av personuppgiftsansvarige. Datainspektionen är den myndighet som i vissa fall kan döma ut en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter.

Interna styrdokument

Interna styrdokument har upprättats för att säkerställa korrekt hantering av personuppgifter inom verksamheten, i enlighet med gällande lagstiftning.

För vidare information om kommunens riktlinjer och rutiner kring dataskyddsarbete, se:

- Informationssäkerhetspolicy
- Rutin för rapportering av personuppgiftsincident
- Rutin vid nya eller förändrade personuppgiftsbehandlingar
- Rutin vid begäran om registerutdrag