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	Kommunfullmäktige 2021-02-24, § 19

Innehållsförteckning

1 Bakgrund

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

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

2 Dokumentation

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

Detta dokument reglerar hur Eda kommun behandlar personuppgifter i enlighet med reglerna i dataskyddsförordningen och dataskyddslagen. Dokumentet omfattar både kommunen och dess bolag. När Eda kommun och/eller kommunen benämns i dokumentet innefattar benämningen även kommunens helägda bolag.

3 Grundläggande definitioner

3.1 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. Det kan även uttryckas som så att en person är identifierbar eller sökbar utifrån de uppgifter som förs.

3.2 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.

3.3 Personuppgiftsansvarig

Personuppgiftsansvarig är en fysisk eller juridisk person eller myndighet som bestämmer ändamålen med och medlen för behandling av personuppgifter. I Eda kommun är respektive nämnd och styrelse personuppgiftsansvarig.

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.

3.4 Personuppgiftsbiträde

Ett personuppgiftsbiträde är en fysisk eller juridisk person som externt hanterar personuppgifter för den personuppgiftsansvariges räkning.

3.5 Personuppgiftsbiträdesavtal

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

3.6 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.

3.7 Dataskyddsombud

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

4 Grundläggande principer för behandling av personuppgifter

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

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 Integritet och konfidentialitet

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

4.7 Ansvarsskyldighet

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

5 Behandling av personuppgifter

5.1 Rättslig grund

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Utöver de grundläggande principerna, ska det finnas en rättslig grund för behandlingen. För kommunens verksamhet ska någon av följande lagliga grunder användas för behandling av personuppgifter:

5.1.1 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. anställningsavtal, avtal med företag och liknande. 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.

5.1.2 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. Obligatoriska uppgifter som ålagts kommunen att utföra är av allmänt intresse. Kommuner har också möjlighet att göra frivilliga åtaganden, t.ex. att förvalta fritids- och idrottsanläggningar; främja ortens näringsliv eller anordna kulturell verksamhet. Uppgifter av allmänt intresse ska ha stöd i lag eller annan författning alternativt i kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.

5.1.3 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. Myndighetsutövning innebär att kommunen har statens uppdrag att bestämma över enskilda medborgare vad gäller exempelvis förmån, rättighet, skyldighet, disciplinpåföljd, avskedande eller annat jämförbart förhållande.

5.1.4 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.

5.1.5 Samtycke

Samtycke ska endast användas i undantagsfall som laglig grund i kommunens verksamhet, och förutsatt att kommunen inte har annan grund som tillåter behandling. Ett samtycke ska vara individuellt, frivilligt, tydligt

och informerat efter det att den registrerade fått information om tilltänkt behandling.

Den registrerade kan återkalla sitt samtycke, vartefter fortsatt behandling inte vidare får ske. Återkallandet påverkar inte lagligheten av behandling som skett före samtycket återkallats.

6 Personuppgifter på kommunens 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 4.4) som ingår i ett justerat protokoll som förts vid ett nämnd-, styrelse-, eller fullmäktigesammanträde får publiceras på kommunens hemsida. Innan materialet läggs ut på hemsidan ska det granskas så att inga integritetskänsliga eller sekretessbelagda personuppgifter publiceras.

6.1 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 sekretess gäller 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.

7 Särskilt om 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.

Ett antal undantag finns i artikel 9 i förordningen där det anges när verksamheten får behandla känsliga personuppgifter. Behandlingen är tillåten om den 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.

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.

8 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.

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.

8.1 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 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. Födelsedatum räknas inte som personnummer och kan skrivas ut på förteckningar om personuppgiftsbehandlingen i övrigt är tillåten.

9 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.

10 Informationskravet och de registrerades rättigheter

Information om en specifik behandling av personuppgifter ska alltid ges till den registrerade. 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.

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 behöver inte lämnas om det finns andra bestämmelser som gäller framför dataskyddsförordningen, t.ex. om vissa uppgifter omfattas av sekretess.

10.1 Klar och tydlig information

Den registrerade har rätt att få tydlig information om vad en personuppgiftsbehandling avser. Vid insamlande av personuppgifter ska den registrerade få information om:

- identitet (vem är det som kräver in personuppgifter?)
- vilka uppgifter som registreras
- ändamål med behandlingen (vad ska uppgifterna användas till?)
- varifrån uppgifterna hämtas
- rättsliga grunder för behandlingen
- hur länge personuppgifterna lagras
- ev. andra instanser som uppgifterna delas med
- 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.

11 Rättigheter för den registrerade

11.1 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 via ett s.k. registerutdrag.

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.

11.2 Rätt till rättelse av personuppgifter

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

11.3 Rätt till radering (”rätten att bli bortglömd”)

Beroende på omständigheter i det enskilda fallet och på vilken rättslig grund som personuppgiftsbehandlingen görs, kan den registrerade 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.

11.4 Information vid personuppgiftsincident

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

12 Kommunens (de personuppgiftsansvarigas) ansvar

Kommunens ansvar 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.

13 Registerförteckning

Dokumentation som på något sätt behandlar personuppgifter ska sammanställas i en registerförteckning. Dataskyddskoordinator inom respektive verksamhet/bolag ansvarar för att upprätta och underhålla verksamhetens/bolagets registerförteckning.

14 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. 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.

15 Säkerhet vid behandling

Grundskyddet för 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. Behörigheter ska kontrolleras regelbundet.

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, samt tidpunkt för behandling.

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

15.1 Kartläggning av integritetsrisker

Kartläggning av integritetsrisker
Vid behandling av personuppgifter som innebär integritetsrisker (t.ex. kameraövervakning, genetiska register eller inom sjukvården) ska en konsekvensbedömning avseende dataskydd upprättas.

Konsekvensbedömningar för känsliga behandlingar genomförs av aktuell verksamhet i samverkan med informationssamordnare, IT-avdelningen och dataskyddsombud. I särskilda fall kan konsekvensbedömningen anmälas till Datainspektionen som gör en förhandskontroll och säkerställer att behandlingen är i enlighet med förordningens regler. Beslut om begäran av förhandssamråd tas av kommunchef.

15.2 Åtgärder vid personuppgiftsincident

En personuppgiftsincident ska så snart som möjligt inom 72 timmar anmälas till Datainspektionen. I somliga fall beslutar Dataskyddsinspektionen att personuppgiftsansvarig ska informera den registrerade om incidenten.

15.3 Användande av personuppgiftsbiträde

Personuppgiftsansvariga ska endast använda sig av personuppgiftsbiträde om det anlitade biträdet 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. Biträdesavtalet ska undertecknas av den som enligt gällande delegationsordning har tilldelats rätt att åt personuppgiftsansvarige underteckna biträdesavtal.

15.4 Överföring av 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.

16 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.

17 Interna styrdokument

Interna styrdokument ska 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 ansvar och organisation för tillämpning av dataskyddsförordningen (GDPR) och dataskyddslagen
- Rutin för rapportering av personuppgiftsincident
- Rutin vid nya eller förändrade personuppgiftsbehandlingar
- Rutin vid begäran om registerutdrag
- Rutin för konsekvensbedömning