KOMMUNKANSLIET

Datum 2023-02-01

Brevnr/Diarienr

Berörda handläggare

Handläggare:
Cornelia Gustafsson

GDPR, General Data Protection Regulation – rutin

Dokumenttyp:	Rutin
Diarienummer:	KK 2020-000079 005
Sammanfattning:	Denna beskrivning syftar till att på en övergripande nivå vägleda medarbetare i Avesta kommun i behandlingen av personuppgifter i enlighet med dataskyddsförordningen – GDPR.
Fastställd av/datum:	Fastställd av koncernledningsgruppen 26 september 2019
Giltighetstid:	Tills vidare
Gäller för:	Avesta kommunkoncern
Reviderad:	2023-xx-xx av kommundirektör
Granskad:	
Dokumentansvarig:	Kommunsekreterare
Webbansvarig:	Utredare

Avesta kommun och GDPR - rutinbeskrivning

Antagna av koncernledningsgruppen 26 september 2019, reviderade 2 februari 2024

Syfte

EU:s dataskyddsförordning (General Data Protection Regulation - GDPR), som trädde i kraft den 25:e maj 2018, gäller som lag i Sverige. Syftet är att skydda den grundläggande mänskliga rättigheten, rätten till ett privatliv. En människas personliga integritet ska inte kränkas i samband med behandlingen av personuppgifter.

Denna beskrivning syftar till att på en övergripande nivå vägleda medarbetare i Avesta kommun i behandlingen av personuppgifter i enlighet med dataskyddsförordningen – GDPR.

Dataskyddsförordningen, GDPR -en beskrivning

Alla behandlingar enligt dataskyddsförordningen, GDPR, måste uppfylla de grundläggande principerna och ha rättslig grund.

Ett av syftena med dataskyddsförordningen, GDPR, är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Dataskyddsförordningen har också till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU.

Alla personuppgiftsbehandlingar måste ha rättslig grund, till exempel avtal (anställningsavtal, avtal med kund), allmänt intresse (forskning, statistik, arkiv) myndighetsutövning (bygglov, ekonomiskt bistånd) och rättsliga förpliktelser (till exempel bokföringsskyldighet).

Alla personuppgifter som på något sätt behandlas i kommunens verksamheter omfattas av GDPR med följande undantag:

- privat behandling, som därmed saknar koppling till yrkes- eller affärsmässig verksamhet,
- uppgifter om avlidna,
- om de strider mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,
- journalistiska ändamål, akademiskt, konstnärligt och litterärt skapande,
- tillgången till allmänna handlingar – offentlighetsprincipen,
- nationell säkerhet och gemensam utrikes- och säkerhetspolitik,
- brottsbekämpande myndigheter.

GDPR omfattar även äldre information om personuppgifter som fanns och behandlades i kommunens verksamheter när förordningen trädde ikraft.

Avesta kommun är skyldig att följa och visa att kommunen följer GDPR, varför det är viktigt att alla anställda och förtroendevalda i kommunen tar ansvar för att personuppgifter hanteras på rätt sätt. Att dokumentera vad man gör och varför är helt avgörande för att kunna visa hur kommunen följer GDPR. En förutsättning för att anställda ska kunna hantera personuppgifter på rätt sätt är också att verksamheterna har och följer en aktuell dokumenthanteringsplan och gallringsbeslut.

Dataskyddsarbetet i organisationen handlar om ett förändringsarbete som ska genomsyra hela verksamheten med att bygga system och processer som uppfyller GDPR:s krav. Det kräver ett proaktivt arbete från styrelsens och ledningens sida och ett gott ledarskap. En modern förvaltning förutsätter ett gott skydd för den personliga integriteten.

Varje verksamhet ansvarar för sina egna personuppgiftbehandlingar. Kraven på IT-system som hanterar personuppgifter är starkt. Personuppgifter ska exempelvis skyddas så att bara de som är behöriga kan se eller arbeta med uppgifterna. Uppgifterna måste även skyddas så de inte förstörs genom olyckshändelse. Ändamålet måste vara tydligt vid insamlingen av uppgifter och du får endast hantera personuppgifter på det sätt som finns angivet i ändamålet. Avesta kommun får inte samla in fler personuppgifter än nödvändigt, till exempel för att "det kan vara bra att ha".

En sanktionsavgift kan utdömas vid överträdelse mot förordningen. Från 1 januari 2021 byter Datainspektionen namn till Integritetsskyddsmyndigheten. Integritetsskyddsmyndigheten är tillsynsmyndighet. Vid överträdelse mot dataskyddsförordningen kan även den eller de drabbade begära skadestånd/ersättning.

Begreppsförklaringar

Personuppgifter

Till personuppgifter räknas all slags information som kan knytas till en fysisk person som är i livet. Exempelvis personnummer, namn, adress, foton, registreringsnummer, fastighetsbeteckning, identifikationer online, personers fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter. Det är som huvudregel förbjudet att behandla känsliga personuppgifter, men det finns undantag. Innan du behandlar känsliga personuppgifter måste du ha klart för dig vilket stöd som finns för behandlingen. Känsliga personuppgifter är uppgifter om 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.

Extra skyddsvärda personuppgifter

Det finns många andra typer av personuppgifter som är särskilt skyddsvärda. Det kan till exempel vara personnummer, löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter; till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, information som rör någons privata sfär, uppgifter om sociala förhållanden. Behandling av extra skyddsvärda uppgifter innebär högre skyddsnivå.

Personuppgiftsbehandling

Med personuppgiftsbehandling menas alla sätt som personuppgifter behandlas på inom en verksamhet. Exempelvis insamling av personuppgifter, spridning, registrering och lagring.

Exempel: kund- och leverantörsregister, attesteringssammandrag, besöksliggare, passersystem, verksamhetssystem, pensionslistor, medarbetarsamtal/lönesamtal, klasslistor, intern telefonkatalog, behörighetsadministration, loggar, hemsida/intranät och rekryteringsdatabas.

Rättslig grund

Utan rättslig grund för behandlingen är personuppgiftsbehandlingen inte laglig. Det finns sju rättsliga grunder varav de sex första rör kommunens verksamhet. Allmänt intresse och myndighetsutövning är de vanligaste rättsliga grunderna i kommunal verksamhet.

Allmänt intresse: Kräver stöd av nationell lagstiftning eller EU-rätt. Måste finnas beskriven och vara tydlig, precis och förutsägbar för den registrerade Ska vara nödvändigt för att utföra en uppgift av allmän karaktär.

Myndighetsutövning: Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter.

Avtal: Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige.

Rättslig förpliktelse: Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet.

Grundläggande intresse: Den personuppgiftsansvarige måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, till exempel om den är medvetslös.

Samtycke: Den registrerade har sagt ja till personuppgiftsbehandlingen. **Obs!** I många fall är det inte lämpligt eller kanske inte ens möjligt att stödja sig på den registrerades samtycke. Överväg

därför alltid först om du kan stödja personuppgiftsbehandlingen på någon av de andra rättsliga grunderna. Samtycke förutsätter frivillighet, ej beroendeställning och möjlighet till återkallande.

Berättigat intresse med intresseavvägning: Får inte användas som behandlingsgrund av offentliga myndigheter utom av bolag i vissa fall.

Information på hemsidan

En övergripande information till allmänheten finns på kommunens hemsida. Den informationen hittar du här: https://www.avesta.se/kommun-demokrati/behandling-av-personuppgifter/. Där finns även en blankett, *Begäran om registerutdrag*, som kan skrivas ut och lämnas till kommunens servicecenter. Se: https://www.avesta.se/globalassets/for-alla-sidor/kommun-och-demokrati/delta-och-paverka/blanketter/begaran-om-registerutdrag.pdf. Den återfinns även som e-tjänst: https://avesta.se/mina-sidor/e-tjanster-och-blanketter/kommun-och-demokrati/.

Under rubriken *Sammanträden, handlingar och protokoll* finns även information om personuppgifter i handlingar och protokoll. Se: https://www.avesta.se/kommun-demokrati/handlingar-protokoll/personuppgifter-i-handlingar-och-protokoll/.

Om du vill informera om hur kommunen hanterar personuppgifter kan följande text användas: ”*Information om hur Avesta kommun behandlar dina personuppgifter och hur du tar tillvara dina rättigheter enligt Dataskyddsförordningen (GDPR – General Data Protection Regulation) finns på Avesta kommuns hemsida* www.avesta.se. *Du kan också kontakta Avesta kommuns servicecenter tel. 0226-64 50 00.*”

Personuppgiftsansvarig och dataskyddsombud

Varje nämnd/bolag är personuppgiftsansvarig för sitt verksamhetsområde. Kommunen har även ett utsett dataskyddsombud för alla nämnder och bolag vilket är ett krav enligt dataskyddsförordningen. Uppdraget som dataskyddsombud innebär att: samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument samt informera och ge råd inom organisationen.

Personuppgiftshandläggare

Varje förvaltning har utsett en personuppgiftshandläggare som bland annat har till uppgift att svara för förvaltningens registerförteckning, dokumentera personuppgiftsarbetet samt stödja enhetscheferna i deras arbete med personuppgiftsfrågor.

Personuppgiftshandläggarna lägger in alla registerbehandlingar som görs på förvaltningen i systemet Draftit/Privacy.

Register

Personuppgiftsansvarig, som i Avesta kommun är ansvarig nämnd eller styrelse ansvarar för sina personuppgiftsbehandlingar. Alla behandlingar ska finnas i ett gemensamt register i Draftit och de olika enheterna/verksamheterna är i sin tur ansvariga för att registret både är kvalitetssäkrat och uppdaterat.

Registret är ett ställt krav från Dataskyddsförordningen, GDPR, som samtidigt ger oss kontroll över vilka personuppgiftsbehandlingar vi utför i kommunen. Det hjälper oss också att, på ett systematiskt sätt, kontrollera att vi till exempel har en rättslig grund att behandla uppgifterna.

Registret är en total kartläggning av alla behandlingar av personuppgifter som utförs inom respektive nämnd eller styrelse.

Åtkomsten till Draftit/Privacy är behörighetsstyrt och varje verksamhet kan endast se sina egna behandlingar.

Respektive enhetschef anmäler behandling inom dennes verksamhetsområde till personuppgiftshandläggare. Personuppgiftshandläggaren ansvarar för att registerförteckningen hålls uppdaterad. Varje behandling ska även uppdateras när nya förutsättningar gäller för dess hantering, såsom till exempel. att den avslutats eller att de informationssäkerhetsmässiga skydden förändrats.

Hur hanteras begäran om registerutdrag?

En privatperson som begär ett registerutdrag från Avesta kommun ska vända sig till kommunens servicecenter. Servicecenter vidarebefordrar därefter begäran till den nämnd varifrån registerutdrag begärs.

Respektive nämnd/förvaltning avgör sedan vem som tar fram uppgifterna inom nämndens område. Lämpligt är att personuppgiftshandläggaren arbetar med frågan. Kommunen har en månad på sig att lämna ut de begärda uppgifterna antingen via servicecenter eller direkt till folkbokföringsadressen. Rutinen är för närvarande att samtliga nämnder/förvaltningar utom omsorgen skickar sitt svar via servicecenter.

Den registrerade har rätt att få information om bland annat om vilka personuppgifterna är, ändamålen med behandlingen, varifrån uppgifterna kommer, till vilka mottagare som uppgifterna har eller kommer att lämnas ut, rätten att begära rättelse eller radering av personuppgifter, rätten att inge klagomål till en tillsynsmyndighet.

E-posthantering – Avesta kommun

E-post som kommer in till kommunen blir normalt en allmän handling som ska registreras eller hållas ordnad. Utgångspunkten är att det är tillåtet att behandla personuppgifter för att uppfylla kraven i arkivlagen om bevarande av allmänna handlingar. Alla e-postmeddelanden är dock inte allmänna handlingar, till exempel privata meddelanden.

E-post får inte användas för att skicka sekretessbelagd information, varken externt eller inom kommunen. Personuppgifter bör i möjligaste mån inte skickas via e-post. Om personuppgifter skickas till dig så ska dessa aldrig vidarebefordras eller finnas kvar i eventuellt svar till den som skickat meddelandet.

Några råd för e-posthantering:

- Sprid inte personuppgifter i onödan. Skicka bara personuppgifter till dem som behöver uppgifterna för sitt arbete och radera meddelandet i mappen skickat och i mappen borttagna objekt.

- Om du tar emot ett meddelande med personuppgifter se till att det överförs till relevant system och radera meddelandet i din inkorg och i borttagna objekt.
- Om du skickar e-post till många samtidigt (rekommenderas inte om det innehåller personuppgifter), överväg om adresserna ska skrivas i fältet ”hemlig kopia”.

Bilder

Publicering av bilder kräver samtycke. Om inte detta finns ska bilderna tas bort eller arkiveras. En e-tjänst för samtycke har tagits fram. Undvik om möjligt bilder där personer går att identifiera.

Personuppgiftsbiträdesavtal

Avesta kommun ska teckna personuppgiftsbiträdesavtal med kunder/leverantörer. Detta under förutsättning att någon av parterna är biträde till den andra. Ibland kan vi använda det personuppgiftsavtal som skickas till oss. Till hjälp finns en checklista för granskning som ligger under adressen G/Kommun/GDPR. Där finns även framtaget ett förslag till personuppgiftsbiträdesavtal som kan användas. Om ni behöver hjälp med granskningen rekommenderas ni att kontakta IT-chefen.

Styrdokument

De styrdokument som reglerar kommunkoncernens dataskyddsarbete är

- digitaliseringspolicy, som antas av kommunfullmäktige,
- informationssäkerhetshandlingsplan, som antas av koncernledningsgruppen
- utbildningsplan, som antas av koncernledningsgruppen
- denna rutinbeskrivning, som antas av koncernledningsgruppen
- riktlinjer för e-posthantering

Respektive förvaltning/bolag kan anta specifika rutiner för sitt område.

Digitaliseringspolicy

En digitaliseringspolicy för Avesta kommunkoncern har antagits av kommunfullmäktige. Här säkerställs att verksamheterna drar åt samma håll när det gäller IT-utvecklingen och digitaliseringen. Inriktningen är följande:

- Kommunkoncernens digitalisering ska ses till att värdet för medborgaren alltid är i fokus
- Verksamheterna ska tänka ”digitalt först” i sin verksamhetsutveckling
- IT-enheten och verksamheterna ska samverka och dela kompetenser för att uppnå samordning både internt och extern
- IT-enheten ska både vara med att stimulera verksamheterna i digitaliseringen samtidigt som att ett fungerade IT-stöd ska levereras.

Dataskyddsprinciperna (proportionalitet, ansvarsskyldighet, ändamålsbegränsning, uppgiftsminimering/relevans, lagringsminimering, korrekthet, integritet/konfidentialitet (behörigheter), öppenhet, laglighet, korrekthet och öppenhet) ska genomsyra all kommunal verksamhet.

Vid organisering och utförande av dataskyddsarbetet ska effektivitet, samordning och samverkan eftersträvas så långt det är möjligt för kommunkoncernen som helhet.

Servicenivån i Kommunkoncernens förvaltningar och bolag ska följa gällande lagstiftning och Kommunkoncernens tjänstegarantier och tillgodose invånarnas fri- och rättigheter utifrån ett GDPR-perspektiv. Servicen ska utmärkas av tillit och uppfattas som välkomnande, trygg och enkel.

Informationssäkerhetshandlingsplan

En informationssäkerhetshandlingsplan för Avesta kommun har tagits fram. Där beskrivs hur arbetet är organiserat samt vilka uppgifter koncernledningsgruppen, IT-gruppen, Administrativa gruppen, personuppgiftshandläggaren, kommunsekreteraren och servicecenter har. I handlingsplanen beskrivs även hur kommunen ska arbeta med utbildning inom området.

Informationssäkerhetsplanen antas av koncernledningsgruppen.

Utbildning

En viktig faktor för GDPR-anpassningen är att medarbetarna kontinuerligt erbjuds utbildning inom GDPR och informationssäkerhet. Koncernledningsgruppen beslutar årligen om en utbildningsplan för kommunens medarbetare.