FALKENBERGS KOMMUN

Riktlinje för hantering av personuppgifter i e-post och kalender

Diarienummer 2018/174	Fastställt av Kommunstyrelsen	Datum för fastställande 2019-01-15
Dokumenttyp Riktlinje	Dokumentet gäller för Samtliga nämnder och bolag	Giltighetstid Tills vidare
Revideringsansvarig * Kommunstyrelsen	Revideringsintervall Vart annat år	Reviderad datum
Dokumentansvarig (funktion) ** Informationssäkerhetssamordnare	Uppföljningsansvarig och tidplan (se punkt 5) Respektive nämnd och styrelse	

Falkenbergs kommun
311 80 Falkenberg. Telefon växel: 0346-88 60 00. Fax: 0346-133 40
e-post: kontaktcenter@falkenberg.se
www.falkenberg.se

1. Syfte

För Falkenbergs kommuns anställda och förtroendevalda är e-post, kalender och där tillhörande tjänster ett nödvändigt arbetsredskap.

Syftet med denna riktlinje är att ange hur Falkenbergs kommuns verksamheter ska hantera personuppgifter i e-post, kalender, kontaktlistor och uppgifter, det som idag är Outlook. Detta för att säkerställa att hanteringen sker i enlighet med gällande lagstiftning.

Riktlinjen omfattar enbart hantering av personuppgifter i e-post, kalender, kontaktlistor och uppgifter. Känsliga, eller extra skyddsvärda personuppgifter skickas över säker digital kommunikation. Se särskild anvisning.

Alla kommunens verksamheter omfattas av denna riktlinje. Respektive nämnd/bolag kan i sin tur anta mer detaljerade anvisningar kring hanteringen av personuppgifter i e-post/kalender och där tillhörande tjänster.

2. Koppling till lagstiftning och andra styrdokument

Denna riktlinje är förenlig med gällande lagstiftning och andra styrdokument. Riktlinjen är underordnad kommunens informationssäkerhetspolicy.

Vilken typ av information som hos myndigheter ska betraktas som allmänna handlingar framgår av tryckfrihetsförordningens andra kapitel. Huvudregeln är att allmänna handlingar är offentliga. Offentlighets- och sekretesslagen specificerar undantagen från denna huvudregel.

Genom EU:s dataskyddsförordning skyddas människor mot att deras personliga integritet kränks vid behandling av personuppgifter. Förordningen innehåller regler om vilka tekniska hjälpmedel och säkerhetsåtgärder som behöver vidtas vid hantering av personuppgifter. Behandling av personuppgifter får endast ske inom ramen för syftet då de samlades in. Uppgifter får inte senare behandlas på ett sätt utöver det ursprungliga syftet och inte heller sparas längre än nödvändigt. Inga onödiga personuppgifter får behandlas. För att hantera personuppgifter krävs rättsligt grund för behandlingen, saknas sådan får personuppgifterna inte behandlas. De rättsliga grunderna för behandling av personuppgifter är:

- Den registrerade har lämnat sitt samtycke.
- Avtal med den registrerade ska kunna fullgöras.
- Den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet.
- Vitala intressen för den registrerade ska kunna utföras.
- En arbetsuppgift av allmänt intresse eller i samband med myndighetsutövning ska kunna utföras.
- Efter en intresseavvägning.

I den mån det finns utrymme för nationella variationer kompletteras dataskyddsförordningen av den svenska dataskyddslagen och den svenska dataskyddsförordningen.

E-post, kalender och där tillhörande tjänster innehåller i princip alltid personuppgifter och omfattas därmed av reglerna inom dataskydd.

Arkivering och gallring regleras i arkivlagen, arkivförordningen och Riksarkivets föreskrifter. Utöver detta finns verksamheternas dokumenthanteringsplaner.

3. Riktlinje

3.1. Privat e-post

Privat e-post får inte hanteras i kommunmailen. För det fall privat e-post ändå kommer in till kommunmailen bör den raderas alternativt flyttas omgående. Du får inte heller nyttja arbetets e-postadress för att i privat syfte registrera dig på webbsidor för exempelvis näthandel, medlemskap eller skapa konto i sociala medier.

3.2. Känsliga, eller extra skyddsvärda personuppgifter

Av dataskyddsförordningen framgår att vissa personuppgifter anses vara känsliga, eller extra skyddsvärda.

Med känsliga personuppgifter avses exempelvis hälsoinformation. Med extra skyddsvärda uppgifter avses exempelvis sekretessbelagd information enligt offentlighets- och sekretesslagen eller personnummer. Se rubrik 4 för ytterligare förklaring av begreppen.

3.3. Skicka personuppgifter

Personuppgifter kan skickas via e-post/kalender så länge de **inte** innehåller uppgifter som är känsliga, eller extra skyddsvärda. Observera att detta gäller såväl internt som externt samt att även bifogade filer och liknande omfattas.

I de fall känsliga personuppgifter, eller extra skyddsvärda uppgifter, behöver kommuniceras digitalt, ska säker kommunikation användas. Se särskild anvisning gällande ”Säker digital kommunikation”.

Undvik att använda och sprida personuppgifter när det inte är nödvändigt. Skicka bara personuppgifter till dem som behöver uppgifterna för sitt arbete/uppdrag. Skicka inga kopior ”för säkerhets skull”.

Om e-post skickas till många mottagare, överväg om adresserna ska skrivas i fältet för hemlig kopia. Detta för att förhindra att mottagarna får kännedom om varandra.

3.4. Motta personuppgifter

Det är innehållet i mottagen e-post som avgör om, och hur länge e-posten får sparas. Innehållet avgör också hur personuppgifterna fortsatt ska behandlas.

Att någon skickar känsliga, eller extra skyddsvärda uppgifter till kommunen innebär inte att denne lämnat samtycke till att personuppgifterna hanteras i e-post/kalender. Den enskilde har ingen information om vilka säkerhetsåtgärder som kommunen har vidtagit för hanteringen och ett samtycke är därför inte aktuellt. Tänk därför på att inte svara genom att skicka med innehåll som exempelvis omfattas av sekretess via e-post. Dessa uppgifter tas bort innan svar skickas, i annat fall ska svar skickas via säker digital kommunikation.

Inkommen e-post med känsliga, eller extra skyddsvärda personuppgifter, får inte förekomma i e-post/kalender. När den här typen av uppgifter kommer in ska de snarast överföras till det system där de hör hemma, exempelvis ett ärendehanteringssystem. De ska även rensas från inkorgen och övriga mappar, såsom exempelvis borttagna meddelanden, skräppost, skickat etc. Papperskorgen ska tömmas.

3.5. Kalender, kontaktuppgifter

Känsliga, eller extra skyddsvärda personuppgifter, får inte förekomma i kalender eller i kontaktuppgifter. Övriga personuppgifter kan hanteras så länge det är nödvändigt för genomförandet av arbetsuppgifter och uppdrag.

3.6. Flytta personuppgifter till andra system

Det är olämpligt att använda e-post/kalender för att behandla personuppgifter långsiktigt. E-post/kalender är ingen säker förvaring och det kan vara svårt att hitta uppgifter om en enskild i e-posten/kalendern eller säkerställa att uppgifterna blir borttagna när de inte längre behövs. Uppgifterna bör flyttas från e-post/kalender till ett lämpligare system, som exempelvis ett ärendehanteringssystem eller kundregister. Observera att känsliga, eller extra skyddsvärda personuppgifter, ska flyttas omgående enligt föregående stycken.

3.7. Gallring

Gallring av handlingar innebär att handlingarna förstörs. Vilka handlingar som får gallras och vilka som ska bevaras framgår av förvaltningens antagna dokumenthanteringsplan.

E-post av mindre betydelse kan raderas omgående. För e-post av betydelse gäller samma regler som för information på papper, dvs. innehållet i e-posten avgör hur handlingen ska hanteras (diarieföras, bevaras, gallras etc.). Det är varje medarbetares/förtroendevalds ansvar att hantera sitt eget konto.

Automatiserad gallring av e-post sker efter 24 månader.

Konton i Outlook gallras enligt kommunstyrelsens dokumenthanteringsplan tre månader efter att de är avslutade dvs. när personen inte längre är kvar i organisationen.

4. Definitioner och avgränsningar

Inom ramen för e-post/kalender innefattas samtliga mappar i e-posten, kalender, kontaktlistor och uppgifter. Såväl intern som extern e-post omfattas liksom arbetsrelaterad e-post som skickas/tas emot via privat e-postkonto.

Med personuppgift avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är om uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Exempel på personuppgifter är namn, bilder på individer och IP-nummer (om de kan kopplas till fysiska personer).

Personnummer består av födelsetid (6 siffror), ett födelsenummer (3 siffror) samt en kontrollsiffra. Födelsetid är inte ett personnummer och därmed inte att betrakta som extra skyddsvärt.

Med behandling avses alla former av åtgärder med personuppgifter, exempelvis insamling, registrering, lagring, ändring, radering, spridning m.m. Alla typer av personuppgiftsbehandlingar ska registreras enligt dataskyddsförordningen.

Med känsliga personuppgifter, eller särskilda kategorier av uppgifter, enligt dataskyddsförordningen, avses uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydligt identifierar en person.

Utöver känsliga personuppgifter förekommer personuppgifter som anses extra skyddsvärda. Med extra skyddsvärda personuppgifter avses i denna riktlinje

- personuppgifter som omfattas av sekretess eller tystnadsplikt (eller annan särlagstiftning, exempelvis patientdatalagen)
- personnummer
- uppgifter om lagöverträdelser.

Med säker digital kommunikation avses ett säkert sätt att utbyta integritetskänslig information samt säkerställa både mottagarens och avsändarens identitet.

Ansvar och uppföljning

Kommunstyrelsen ansvarar för att ta fram, och revidera denna riktlinje.

Varje nämnd och styrelse ansvarar för att behandling av personuppgifter inom respektive verksamhetsområde följer gällande lagstiftning och övriga styrdokument inom området.

Enligt dataskyddsförordningen är respektive nämnd och styrelse personuppgiftsansvarig för sin behandling av personuppgifter. Respektive nämnd och styrelse ansvarar för att denna riktlinje följs. I detta ansvar ligger att informera samtliga anställda, förtroendevalda och uppdragstagare om detta dokument samt följa upp efterlevnaden av riktlinjen.