Falkenbergs kommun

Riktlinje för hantering av personuppgifter i e-post och kalender

Diarienummer KS 2025/292	Fastställd av Kommunstyrelsen	Datum för fastställande 2019-01-15
Dokumenttyp Riktlinje	Dokument gäller för Alla nämnder och helägda bolag	Giltighetstid Tills vidare
Revideringsansvarig Kommunstyrelsen	Revideringsintervall Vart fjärde år	Reviderat datum 2025-12-02
Dokumentansvarig (funktion) Säkerhetschef	Uppföljningsansvarig Respektive nämnd och styrelse	Uppföljning Inom ramen för intern kontroll och revision

Falkenbergs kommun
31180 Falkenberg. Telefon kontaktcenter: 0346-88 60 00.
e-post: kontaktcenter@falkenberg.se
kommun.falkenberg.se

Falkenbergs kommun

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, oberoende av vilket IT-system eller digital tjänst som används. 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 genom säker digital kommunikation. Information om säker digital kommunikation finns på intranätet.

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 säkerhetspolicy.

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. Personuppgifter får endast samlas in och behandlas för tydligt angivet syfte och får inte sparas längre än nödvändigt. Endast nödvändiga uppgifter ska hanteras och behandlingen ska alltid skydda individens integritet genom lämpliga säkerhetsåtgärder. Behandling kräver rättslig grund som till exempel ett avtal, rättslig förpliktelse eller uppgift av allmänt intresse/myndighetsutövning.

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

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 informationshanteringplaner.

3 Riktlinje

3.1 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 personnummer, integritetskänsliga uppgifter som rör personliga/sociala förhållanden. Se rubrik 4 för ytterligare förklaring av begreppen.

3.2 Lagring och kommunikation av personuppgifter

Personuppgifter ska alltid hanteras på ett sätt som skyddar den enskildes integritet. För detta finns vägledning på intranätet som anger vilka lagringsytor och kommunikationskanaler som ska användas beroende på uppgifternas skyddsvärde.

Det är olämpligt att använda e-post/ och kalender för att behandla personuppgifter långsiktigt. E-post och kalender är ingen säker förvaring och det kan vara svårt att hitta uppgifter om en enskild i e-posten och kalendern eller säkerställa att uppgifterna blir borttagna när de inte längre behövs.

Känsliga och extra skyddsvärda personuppgifter får inte lagras i e-post eller kalender. Flytta dem direkt till ett verksamhetssystem eller annan godkänd säker lagringsyta. Känsliga och extra skyddsvärda personuppgifter kommuniceras genom säker digital kommunikation.

Notera att detta även innebär att känsliga personuppgifter eller extra skyddsvärda personuppgifter inte får skannas till användares inkorg via e-post. Skanning av känsliga personuppgifter eller extra skyddsvärda personuppgifter ska i stället ske till inloggades hemkatalog på en skrivare med funktionen ”Säker skanning”.

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.
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.

Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser eller att vidarebefordra till den privata e-postadressen.

3.3 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 känsliga eller extra skyddsvärda personuppgifter 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 ska snarast föras över 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.

3.4 Kalendrar, 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.

3.5 Gallring

Gallring av handlingar innebär att handlingarna förstörs. Vilka handlingar som får gallras och vilka som ska bevaras framgår av nämndens informationshanteringsplan.

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.

E-postkonto i Outlook och i säkra meddelanden gallras enligt kommunstyrelsens informationshanteringsplan.

4 Definitioner, hänvisningar och avgränsningar

Inom ramen för e-post/kalender innefattas samtliga mappar i e-posten, kalender, kontaktlistor och uppgifter oberoende av vilket IT-system eller digital tjänst som används. 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 med mera. Alla typer av personuppgiftsbehandlingar ska registreras enligt dataskyddsförordningen.

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

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

Utöver känsliga personuppgifter förekommer personuppgifter som anses integritetskänsliga och extra skyddsvärda och i denna riktlinje avses bland annat följande personuppgifter som sådana;

- personnummer
- uppgifter om lagöverträdelser
- löneuppgifter
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

Personuppgifter om barn anses särskilt skyddsvärda i dataskyddsförordningen. Det innebär inte att uppgifter om barn aldrig får skickas via e-post eller förekomma i en kalender. En sammantagen bedömning måste göras i det specifika fallet om vad som är lämpligt eller inte att skicka via e-post och givet att det inte uppenbart handlar om känsliga personuppgifter eller skyddsvärda uppgifter enligt exemplen ovan.

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

5 Ansvar och uppföljning

Kommunstyrelsen ansvarar för att leda, samordna och utveckla kommunens strategiska informationssäkerhetsarbete.

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

Falkenbergs kommun

Enligt dataskyddsförordningen är varje nämnd och styrelse personuppgiftsansvarig för den behandling som sker inom det egna ansvarsområdet. De ska säkerställa att denna riktlinje följs genom att informera berörda medarbetare, förtroendevalda och uppdragstagare samt följa upp efterlevnaden. Varje nämnd och styrelse har en utsedd personuppgiftssamordnare som fungerar som stöd i arbetet.

En grundprincip i GDPR är ansvarsskyldighet. Ansvarsskyldighet innebär att nämnder och förvaltningar fortlöpande ska kunna visa att personuppgifter behandlas enligt GDPR:s krav. Detta förutsätter återkommande uppföljning av rutiner, system och säkerhetsåtgärder. Vid riskfylld behandling krävs särskilt noggrann kontroll.

Dataskyddsombudet roll är att stödja och granska personuppgiftsansvarig i frågor om dataskydd.

Varje medarbetare och förtroendevald ansvarar för att följa gällande styrdokument för informationssäkerhet samt rapportera informationssäkerhetsrelaterade brister och incidenter.