



Riktlinje för hantering av personuppgifter i övergripande ekonomisystem

Diarienummer 2019/132	Fastställt av Kommunstyrelsen	Datum för fastställande 2020-04-14
Dokumenttyp Riktlinje	Dokumentet gäller för Samtliga nämnder och bolag	Giltighetstid Tills vidare
Revideringsansvarig Kommunstyrelsen	Revideringsintervall Vart 4:e år	Reviderad datum
Dokumentansvarig (funktion) Redovisningschefen	Uppföljningsansvarig och tidplan (se punkt 5) Samtliga nämnder inom respektive verksamhetsområde.	



1. Syfte

Syftet med denna riktlinje är att ange hur Falkenbergs kommuns verksamheter ska hantera personuppgifter i ekonomisystem och tillhörande administration. Detta för att säkerställa att hanteringen sker i enlighet med gällande lagstiftning.

Alla kommunens verksamheter omfattas av denna riktlinje. Respektive nämnd/bolag/kommunalförbund kan i sin tur anta mer detaljerande anvisningar kring hanteringen av personuppgifter i sitt egna ekonomi-administrativa arbete.

2. Koppling till lagstiftning och andra styrdokument

Denna riktlinje är förenlig med gällande lagstiftning och andra styrdokument.

Riktlinjen utgår ifrån EU:s dataskyddsförordning (GDPR) som syftar till att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter. I den mån det finns utrymme för nationella variationer kompletteras dataskyddsförordningen av den svenska dataskyddslagen och den svenska dataskyddsförordningen.

För att personuppgifter ska kunna behandlas krävs laglig grund. I denna riktlinje hänvisas till två olika typer av laglig grund art 6 e och f i GDPR;

6e) Allmänt intresse eller myndighetsutövning;

Allmänt intresse

Uppgifter av allmänt intresse ska ha stöd i

- Lag eller annan författning
- Kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning

Myndighetsutövning

Behandlingen av personuppgifter ska vara nödvändig för att kunna utföra sådan myndighetsutövning som är fastställd enligt svensk rätt eller EU-rätt.

Med myndighetsutövning så menas den verksamhet som typiskt sett myndigheter utövar över medborgare, såsom hantering av ärenden om förmåner, rättigheter, skyldigheter, disciplinära bestraffningar eller annat jämförbart förhållande.

6f) berättigat intresse

I fall där personuppgiftsbehandling är nödvändig för ett ändamål som rör ett berättigat intresse, och där den registrerades intresse av skydd för sina personuppgifter inte väger tyngre, i de fallen kan denna rättsliga grund användas. Generellt sett så kan myndigheter sällan tillämpa denna grund men i fall som rör den interna ”kring- administrationen” inom en kommun, t ex fakturahantering, och den därmed förekommande personuppgiftsbehandlingen, då kan denna rättsliga grund nyttjas.

En kommuns informationshantering, inkl. fakturor, styrs av en mängd nationella lagar.

Tryckfrihetsförordningen, TF, styr regelverket kring allmänna handlingar och offentlighetsprincipen. Offentlighets- och sekretesslagstiftningen, OSL, styr vilka handlingar som inte är offentliga.



Arkivering och gallring av information regleras både i bokföringslagen, Arkivlagen, AL, arkivförordningen och Riksarkivets föreskrifter. Utöver detta finns verksamheternas dokumenthanteringsplaner.

Ekonomisystemets kund-, leverantörs- och användarregister innehåller i många fall personuppgifter och omfattas därmed av dataskyddsförordningens regler. Dock gäller bokföringslagens och kommunallagens föreskrifter, liksom skatteverkets regelverk, vad gäller ekonomiska underlag samt krav på transparens.

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

Andra styrdokument som bör tas i beaktande vad gäller hanteringen av fakturor, verifikat och underlag är kommunens informationssäkerhetspolicy samt riktlinjer för hantering av personuppgifter i e-post.

3. Riktlinje

3.1. Inledning

Det är en nödvändighet att hantera personuppgifter i Falkenbergs kommuns ekonomisystem. Kundregistret innehåller personuppgifter på de medborgare som använder kommunens tjänster, leverantörsregistret innehåller, utöver uppgifter om leverantörer till kommunen, även personuppgifter på de anställda och medborgare (som t.ex. elever) som har rätt till ersättning för privata utlägg, och användarregistret innehåller personuppgifter på anställda. Det är viktigt för kommunen att hantera dessa uppgifter i enlighet med både bokföringslagens och dataskyddsförordningens gällande regelverk.

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 eller facktillhörighet. I ekonomisystemet ska inga fakturor, verifikat eller underlag innehållande känslig information registreras, utöver om det inte på annat sätt är möjligt att uppfylla annan lagstiftnings krav.

Med extra skyddsvärda uppgifter avses exempelvis sekretessbelagd information enligt offentlighets- och sekretesslagen eller personnummer. I ekonomisystemet ska inga fakturor, underlag eller verifikat innehållande sekretessbelagd information eller personnummer registreras, utöver om det inte på annat sätt är möjligt att uppfylla annan lagstiftnings krav. Ett exempel på sådan avvikelse är fakturor från enskilda firmor där organisationsnumret även är personnumret.

Det är upp till respektive verksamhet att se till att inte mer information än regelverket kräver registreras i ekonomisystem i form av fakturor, verifikat och underlag.



3.3. Tillgänglighet, behörighet och gallring

Ekonomisystem förhåller sig till bokföringslagen vad gäller lagringstid, vilket gör det möjligt att se historiska händelser i systemet. Endast de personer som utifrån sin tjänsts arbetsuppgifter behöver ha tillgång till ekonomisystem ska ha behörighet. Det är upp till respektive verksamhet att tillse att endast de som behöver har behörighet till ekonomisystem. Fakturor som innehåller personuppgifter, av sådan anledning nämnd i 3.2, ska sekretessmarkeras. Det är mottagande verksamhets ansvar att sekretessmarkera.

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

3.4. Uppgiftsminimering

Undvik att använda personuppgifter i ekonomisystem, samt i intern kommunikation kring ekonomisystem, när det inte är nödvändigt. Skicka bara personuppgifter till dem som behöver uppgifterna för sitt arbete/uppdrag, samt endast genom de kanaler övriga riktlinjer och anvisningar förordar.

3.5. Skicka personuppgifter

Fakturor, verifikat och underlag som innehåller personuppgifter kan skickas via e-post 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, ändå behöver skickas ska ärendesystemet Raindance Helpdesk eller annat verktyg för säker digital kommunikation (för närvarande Säkra meddelanden) användas.

4. Definitioner och avgränsningar

Inom ramen för ekonomisystem innefattas kund- och leverantörsfakturor, verifikat, bokföringsunderlag, information från försystem, upplägg av nya kunder, leverantörer och användare, samt all kommunikation rörande något av ovanstående.

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 födelsedatum (6 siffror), ett födelsenummer (3 siffror) samt en kontrollsiffra. Födelsedatum är inte ett personnummer och därmed inte att betrakta som extra skyddsvärt.

Personuppgifterna kan delas in i följande kategorier;



- Harmlösa personuppgifter
T ex namn, adress, fastighetsbeteckning, telefonnummer, e-postadress, IP-nummer mm.
Som regel harmlösa var och en för sig. MEN, de kan behöva hanteras med försiktighet då det handlar om personuppgift i form av t.ex. foto, film, ljud av identifierbara personer.
Likaså kan en eller ett par harmlösa personuppgifter som hanteras i stora volymer d.v.s. uppgifter om 1000-tals individer eller fall där ett stort antal olika harmlösa personuppgifter rör ett fåtal personer (d.v.s. mycket information per individ) behöva hanteras med försiktighet.
 - Särskilda kategorier (även kallade känsliga personuppgifter)
T ex biometriska och genetiska uppgifter, etnicitet/ras, facklig-, politiska och filosofiska åsikter, hälsouppgifter, sexuell läggning. Begreppen är hämtade från artikel 9 i GDPR
 - Extra skyddsvärda
 - Personnummer
 - Personuppgifter som rör lagöverträdelser, artikel 10 GDPR; generellt gäller ett förbud mot att registrera uppgifter om brott. Myndigheter har dock rätt att registrera information om brott, men bara om det är nödvändigt och berättigat för verksamheten. För övriga organisationer är det förbjudet. Uppgifter om brott behandlas i artikel 10 GDPR som lyder: Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades och rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.”
 - Uppgifter om barn
Artikel 8 GDPR; alla personuppgifter som direkt eller indirekt är hänförliga individer som är yngre än 18 bör behandlas som extra/mer skyddsvärda uppgifter. Personuppgifter om barn anses särskilt skyddsvärda eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och att förstå vilken rätt till skydd för sina uppgifter som de har. Dock; det beror ju på i vilket sammanhang som uppgift om barn förekommer samt vilka uppgifterna är.
 - Övriga integritetskänsliga personuppgifter
T ex värderande uppgifter - utvecklingssamtal, personlighetstester, information som rör någons privata sfär, uppgifter om sociala förhållanden – bör hanteras varsamt, tänka till vid hantering osv.



5. Ansvar och uppföljning

Ekonomiavdelningen ansvarar för att ta fram, och revidera denna riktlinje, samt få mandat att ta fram anvisningar med förslag på hantering i praktiken tillsammans med nämnderna för att kunna följa denna riktlinje.

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

Enligt dataskyddsförordningen är varje nämnd, styrelse och direktion personuppgiftsansvarig för behandling av personuppgifter. Respektive nämnd, styrelse och direktion ansvarar för att denna riktlinje följs. I detta ansvar ligger att informera samtliga anställda, förtroendevalda och uppdragstagare om detta dokument. Efterlevnaden av riktlinjen ska följas upp regelbundet.