RIktlinje
Process: 2.13.6 RGK Hantera informations- och IT-säkerhet
Område: Administrativt stöd
Giltig fr.o.m: 2020-02-14
Giltig t.o.m: 2022-03-11
Faktaägare: Peter Wulff, Informationssäkerhetsstrateg
Fastställd av: Ulrika Gustafsson, Kanslidirektör
Revisions nr: 3
Identifierare: 20757

REGION KRONOBERG

Överföring av sekretessbelagd och integritetskänslig information

Krav vid överföring av känslig information via post, e-post och fax eller överföring på annat elektroniskt sätt.

Innehållsförteckning

1 Inledning

Information är en av Region Kronobergs viktigaste resurser. Att vi kan hantera information korrekt och säkert är därför av yttersta vikt!

Lagar, föreskrifter och myndigheter kräver att information som är sekretessbelagd ska hanteras på ett säkert sätt. Med sekretessbelagd information avses till exempel vårdinformation, personuppgifter, företagsuppgifter eller leverantörsuppgifter i upphandlingar.

Även information som inte är sekretessbelagd kan vara mycket känslig när den handlar om en enskild person. Exempelvis kan uppgifter om en anställds förhållanden, personnummer eller andra personuppgifter upplevas som känsliga för den enskilde.

Även uppgifter om många personer i samma register kan göra att uppgifterna blir känsliga.

För att kunna hantera känslig information på rätt sätt måste säkerhets- och sekretessrutiner vara välkända hos användarna.

Följande fyra kriterier ska alltid vara uppfyllda vid överföring av personuppgifter:

1) **Rätt adressat/mottagare.**
2) **Rätt skyddsåtgärder vid överföring.**
3) **Rätt skyddsåtgärder vid mottagande.**
4) **Rätt rutiner för hur post/meddelanden tas om hand efter mottagandet.**

2 Legala krav

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40 3 kap. 2 § 3p, föreskriver att vårdgivare ska säkerställa att obehöriga inte ska kunna ta del av personuppgifter.

GDPR ställer i artikel 32 krav på rätt skyddsåtgärder vid behandling av personuppgifter. GDPR ställer inga explicita krav utan det är upp till den Personuppgiftsansvarige att i varje behandling av personuppgifter använda rätt skyddsåtgärder. Särskilt viktigt är det att skydda behandling av känsliga personuppgifter.

Känsliga personuppgifter enligt GDPR är uppgifter om:

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa

- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person.

Ett personnummer anses av Datainspektionen vara en extra skyddsvärd personuppgift. Datainspektionen anser därför att personnummer bör exponeras så lite som möjligt.

Krav på rätt skyddsåtgärder gäller oavsett om handlingar eller uppgifter, skickas digitalt eller överförs i pappersform mellan personer/funktioner.

Digital överföring omfattar överföring via:

- Nätverk
- Internet
- e-post
- Fax
- Mobiltelefoni (exempel sms och mms)
- Annan media (exempelvis CD-skiva eller USB).

Innan överföring av information ska alltid menprövning ske, enligt lagen om offentlighet och sekretess.

Mer informations finns i riktlinjerna för:

- ✓ *Utlämnande av allmän handling*
- ✓ *Utlämnande av journal*

3 Rutinbeskrivningar

Det åligger verksamhetschef eller motsvarande att se till att dessa rutiner följs.

3.1 Traditionell postgång

När sekretessbelagda handlingar skickas med traditionell post (Postnord), internt eller externt, ska försändelsen skickas som REK samt i sådana kuvert som inte går att se igenom. Avsändaren ska se till att kuverten är väl förslutna och har korrekt mottagaradress.

Mer informations finns i riktlinje och rutin för:

- ✓ *Traditionell postgång – vårdinformation/allmänna handlingar*

3.1.1 Rutiner för intern post

Kontrollera alltid att det står korrekt och tydlig adress. Vid osäkerhet hämta adressen i verksamhetskatalogen.

3.1.2 Rutiner för extern post - medborgare

Extern post med sekretessbelagd och/eller integritetskänslig information till *medborgare* ska skickas som rekommenderad (REK) post eller med postförskott där brevet vid utlämnande kvitteras ut av mottagaren mot uppvisande av legitimation.

Folkbokföringsadress ska som huvudregel användas, undantag kräver att mottagaren vid överenskommelsen om alternativ adress har legitimerat sig.

Externkuvert ska vara försedda med Region Kronobergs logotyp och korrekt avsändaradress för det fall det kan bli fråga om att försändelsen kommer i retur.

Post till personer med skyddade personuppgifter ska alltid skickas till Skatteverkets förmedlingsuppdrag, gäller även rekommenderad (REK) post.

3.1.3 Rutiner för extern post – myndigheter eller andra vårdgivare

Extern post med sekretessbelagd och/eller integritetskänslig information till *myndigheter* ska skickas som rekommenderad (REK) post.

På kuvertet ska **myndighetens namn stå överst**, därefter tjänstemannens namn, följt av adressen.

Externkuvert ska vara försedda med Region Kronobergs logotyp och korrekt avsändaradress för det fall det kan bli fråga om att försändelsen kommer i retur.

3.1.4 Post till person med Skyddad identitet

Skatteverket åtar sig att förmedla post till personer med skyddade personuppgifter. All post som ska förmedlas ska sändas till Skatteverkets särskilda postförmedlingsadresser.

Mer informations finns i riktlinje och rutin för:

- ✓ *Post till personer med skyddade personuppgifter*

3.2 Elektronisk överföring/utlämnade i digital form

Vid överföring eller utlämnande av sekretessbelagd och integritetskänslig information i digital form (datafil, elektroniskt dokument, register etc.) ska denna vara **skyddad mot insyn och endast läsbar av avsedd/behörig mottagare (kryptering)**.

Detta gäller oavsett hur informationen kommuniceras; om det sker som datafil över öppet nätverk (Internet), om den skickas på CD/USB i kuvert med vanlig post eller intern post, eller ligger på en bärbar dator.

Överfört objekt ska hos mottagaren vara skyddat för obehörig åtkomst och endast åtkomligt för behörig användare genom stark autentisering och/eller genom dekryptering.

Det krävs inte att uppgifterna är krypterade om utlämnandet avser en enskild person och skickas till denne med traditionell postgång på digitalt media, exempelvis CD istället för på papper. Säkerheten med rekommenderat brev eller postförskott anses i detta fall tillräckligt.

3.3 E-post

Sekretessbelagda eller känsligt personuppgifter enligt GDPR kan med nuvarande skyddsnivå inte tillåtas att e-postas då dessa typer av uppgifter kräver ”säker e-post”.

Med ”säker e-post” avses funktioner där e-post skickas krypterat/insynsskyddat för obehöriga och där mottagaren säkert kan identifiera vem som är avsändaren.

Mer information finns i riktlinjer och rutinen:

- ✓ *Regler för e-post*

3.4 Mobiltelefoni inklusive sms/mms

Dataöverföring till och från mobiltelefoner (även sms/mms) sker över ett öppet nätverk och kräver därför att känsliga uppgifter överförs krypterade och endast läsbara för avsedd mottagare.

För att möjliggöra sms-påminnelser har den rättsliga grunden samtycke används. Detta innebär att den registrerade har sagt ja till personuppgiftsbehandlingen.

För att kunna använda den rättsliga grunden samtycke har Datainspektionen ett antal krav, e x v att det ska finnas ett alternativ för de som väljer att avstå samt att det ska vara enkelt att ta tillbaka sitt samtycke.

Mer information finns i rutinen:

- ✓ *Rutin Reminders (påminnelser via e-post och sms från Cosmic)*

3.5 Fax

Överföring av fax sker över ett öppet nätverk och kan därför inte användas för sekretessbelagda eller känsligt personuppgifter enligt GDPR.

I undantagsfall kan man använda fax men då tillsammans med skyddsåtgärderna avidentifikation och motringning.

Mer information finns rutinen:

- ✓ *Faxa sekretessbelagda eller integritetskänsliga uppgifter*