Regiondirektören

BESLUT

Alf Jönsson
Tfn: +46 44 309 31 21
Mail: alf.jonsson@skane.se

Datum: 2018-10-15
Dnr: 1800025

Instruktion för hantering av skyddade personuppgifter

Syftet är att beskriva hur personuppgifter tillhörande personer med skyddade personuppgifter ska hanteras i Region Skåne.

Härmed beslutas att

- ”Instruktion för hantering av skyddade personuppgifter” fastställs
- ”Anvisning – Skyddade personuppgifter” daterad 2012-10-16, upphävs.
- Informationssäkerhetschefen har uppdraget att uppdatera instruktionen och genomföra ändringar med mindre påverkan.

Alf Jönsson
Regiondirektör

Koncernkontoret
Enheten för säkerhet och intern miljöledning

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

Instruktion för hantering av skyddade personuppgifter

Bakgrund

Uppgifter inom folkbokföringsverksamheten är i regel offentliga men sekretess gäller om det av särskild anledning kan antas att en person, eller någon närstående, kan lida skada eller men om uppgifter om personen lämnas ut. I sådana fall kan sekretesskydd tillgripas. Skyddade personuppgifter är det samlingsnamn som Skatteverket använder för de olika sekretesskydden sekretessmarkering, kvarskrivning och fingerade personuppgifter för personer som lever under hot/förföljelse.
Endast folkbokförda personer kan få skyddade personuppgifter. Personer med samordningsnummer eller som är asylsökande kan inte ha skyddade personuppgifter hos Skatteverket.

Legala krav

I **offentlighets- och sekretesslagen (OSL) (SFS 2009:400)** regleras användningen av ”sekretessmarkering”. Person som är utsatt för hot kan hos Skatteverket få en markering om sekretess (sekretessmarkering) i folkbokföringsregistret. Även person som genomgått könsbyte kan erhålla sekretessmarkering. Sekretessmarkering löper ett år, därefter görs ny prövning. Skyddet beslutas av Skatteverket. Markeringen ska fungera som en varningssignal för att uppmärksamma att en prövning ska göras innan några uppgifter om personen lämnas ut.

Folkbokföringslagen (SFS 1991:481) reglerar skyddet ”kvarskrivning”. Kvarskrivning tillgrips då sekretessmarkering inte ger tillräckligt skydd och innebär att personen är kvarskriven på den gamla orten men bor på helt annan ort och i allmänhet i annat län. Kvarskriven är i folkbokföringsregistret registrerad med sitt personnummer men på en särskild adress, s.k. förmedlingsuppdragsadress. Den nya (faktiska) adressen registreras inte i folkbokföringen utan förvaras manuellt på Skatteverket, vilket således innebär att den inte förekommer i Region Skånes befolkningsregister eller kan sökas i Skatteverkets befolkningsregister (Navet). Vid sökning på personnummer visas endast att personen har sekretesskydd. Kvarskrivning löper i högst tre år, därefter görs ny prövning. Skyddet beslutas av Skatteverket. Kvarskriven får sedan 2003 även sekretessmarkering. Kvarskriven har rätt att få vård var han/hon än befinner sig.

Lagen om fingerade personuppgifter (SFS 1991:483) reglerar skyddet ”fingerade personuppgifter” (identitetsbyte) som tillgrips vid särskilt allvarliga hot. Personen får då helt nytt personnummer och nytt för- och efternamn och kan leva med detta under begränsad tid eller under hela sin livstid. Skyddet tilldelas av Skatteverket efter beslut av Polismyndigheten. Fingerade personuppgifter är i allmänhet offentliga, men sekretesskyddet ”sekretessmarkering” kan förekomma.

Av **Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning** (2004) framkommer att en person med sekretessmarkerade personuppgifter bör vara mycket noga med att själv kontrollera om en uppgift som lämnas är sekretesskyddad hos myndigheten. Det framkommer också att det ligger ett ansvar på den enskilde att själv upplysa om eventuell sekretessmarkering eftersom det inte åligger en myndighet att utan anledning kontrollera om en person har sekretessmarkering i folkbokföringen.

Läs mer om sekretesskydden på www.skatteverket.se / Folkbokföring / Skyddade personuppgifter

Socialstyrelsens författning Journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) ålägger alla vårdgivare att ha rutiner som säkerställer att det är möjligt att föra patientjournal när en patient har skyddade personuppgifter.

Utöver ovanstående finns också generella krav på identitetskontroll av patienter och personal när olika verksamheter i landsting/region så kräver att de ska uppvisa legitimation. Detta gäller även för personer som har skyddade personuppgifter.

Skatteverkets förmedlingsuppdrag

Skatteverket ger service till myndigheter och andra organisationer som vill nå en skyddad person genom att vidarebefordra postförsändelser till denne. Avsändaren behöver inte veta var i landet personen är folkbokförd utan kan skicka försändelsen till närmaste förmedlingskontor. Sådan post skickas till **Skatteverket, Förmedlingsuppdrag, Box 2820, 403 20 GÖTEBORG**.

Även om det åligger ett ansvar på den enskilde att upplysa om sin sekretessmarkering kan det ibland behöva konstateras vilket sekretesskydd personen har, detta gäller speciellt inom hälso- och sjukvården när personen också har skyddet kvarskrivning. För att kontrollera om en person har skyddade personuppgifter kan man vända sig till Skatteverkets servicetelefon 0771-567 567, och begära Förmedlingsuppdrag.

Postförmedling

Det brev som ska förmedlas ska läggas i ett innerkuvert som ska ha uppgift om avsändaradress inklusive uppgift om förvaltning och Region Skånes logotyp så att Skatteverket kan returnera försändelsen om verket inte kan nå mottagaren. På kuvertet ska skrivas namnet på mottagaren (för- och efternamn) samt personnummer. Kuvertet läggs sedan i ett ytterkuvert som endast behöver ha Region Skånes logotyp och adresseras till Skatteverket enligt ovan.

Observera att Skatteverket inte har med innehållet att göra varför ett innerkuvert ska vara väl förslutet. Vidare ska observeras att försändelser som skickas till Skatteverket Förmedlingsuppdrag inte ska vara rekommenderade. För att kunna motta rekommenderade brev kräver nämligen Förmedlingsuppdrag direktadressering till mottagaren jämte utskrift av mottagarens personnummer på kuvertet. Detta förfaringssätt är emellertid inte förenligt med de legala krav som styr utlämnande av sekretessbelagd och integritetskänslig information.

Observera också att all förmedlingspost kommer fram någon dag senare till mottagaren än om den skulle ha skickats direkt till mottagaren.

Handläggning - ansvar

Verksamhetschef/motsvarande

Verksamhetschef/motsvarande ska se till att dessa instruktioner görs kända och ska utse en kontaktperson i dessa frågor.

Systemansvarig

Systemansvarig ska se till att IT-stöd kan hantera skyddade personuppgifter. Koppling ska finnas mellan Skatteverkets befolkningsregister och Region Skånes system. Skatteverkets regelbundna aviseringar innehåller även sekretessmarkering. Detta ska kunna tas omhand i IT-stöd i Region Skåne så att skyddad uppgift inte är synlig och/eller att detta signaleras för personal.

Nedan följer rutinbeskrivningar för hantering av patienters respektive anställdas skyddade personuppgifter.

Hantering av patienter med skyddade personuppgifter

Vid sekretessmarkering

- Personnummer och namn ska användas i patientjournal eller annat system som hanterar patientuppgifter även för personer med sekretessmarkering.
- Då patienten uppger sig ha sekretessmarkering och detta inte framgår av systemet ska uppgift kontrolleras i PASiS eller befolkningsregistret. Finns inte uppgift om sekretessmarkering kontakta Förmedlingsuppdrag enligt ovan för att säkerställa att skyddade personuppgifter föreligger.

- Registrera eller dokumentera *inte* sekretessmarkerad patients tillfälligt lämnade telefon eller adressuppgifter vare sig i PASiS, patientjournal eller annat system som hanterar patientuppgifter. Behövs sådana uppgifter för vården av patienten ska de förvaras avskilt och inlåsta samt hanteras av ett fåtal behöriga personer på vårdenheten.
- Överenskom med patienten om meddelandeform, endera att vårdenheten meddelar sig skriftligen via Förmedlingsuppdrag eller informera patienten om telefonnummer till vårdenheten, dit han/hon kan vända sig för besked om provsvar, inläggning mm.
- Meddelas via Förmedlingsuppdrag ska förmedlanderutinerna ovan följas.

Vid kvarskrivning

- Personnummer och namn ska *inte* användas vare sig i patientjournal eller annat system som hanterar patientuppgifter för personer med kvarskrivning.
- Vid behov kontakta Förmedlingsuppdrag för att kontrollera kvarskrivningsskyddet.
- Registrera i PASiS och i patientjournal med reservnummerrutinen; *uppskattat födelseår (ÅÅ) + dagens datum(MMDD)*.[1] I namnfältet registreras OID PERSON och i adressfältet SEKRETESSKYDD. Den kvarskrivna ska ha information om sitt reservnummer och visa upp detta i fortsatta kontakter med regionens vårdverksamheter. Koppling mellan personnummer och reservnummer kan behövas vid identifiering och Förmedlingsuppdrag. Kopplingen ska förvaras åtskilt och inlåst och endast hanteras av ett fåtal behöriga personer på vårdenheten.
- Registrera eller dokumentera *aldrig* kvarskriven patients tillfälligt lämnade telefon- eller adressuppgifter vare sig i PASiS, patientjournal eller annat system. Behövs sådana uppgifter för vården av patienten ska de förvaras avskilt och inlåst samt hanteras av ett fåtal behöriga personer på vårdenheten.
- Informera patienten om telefonnummer till vårdenheten, dit patienten kan vända sig för besked om provsvar, inläggning m.m. Vill den kvarskrivna att vården ska kommunicera med honom/henne via Förmedlingsuppdrag ska detta vara överenskommet och dokumenteras i patientens journal.
- För att underlätta för kvarskriven i fortsatta kontakter med hälso- och sjukvården ska epikris/motsvarande sammanfattning överlämnas till patienten i samband med vårdtillfälle eller öppenvårdsbesök.
- Informera patienten om, att om patienten efter hävd kvarskrivning vill få sitt reservnummer sammankopplat med personnummer ankommer det på patienten att själv kontakta Region Skåne för detta.
- Reservnummer kan inte användas vid kommunikation av personuppgifter mellan annan vårdgivare eller gentemot apotek. Vid debitering av vård till hemlandsting eller vid förskrivning av elektroniskt recept måste därför kvarskrivens personnummer användas. Det ska då utväxlas på ett säkert sätt så att det inte röjs för utomstående.

Vid fingerade personuppgifter

Polis bistår dessa personer i deras kontakter med hälso- och sjukvården. Fingerade personuppgifter ser ut som vilka folkbokföringsuppgifter som helst och registreras därför på sedvanligt sätt i PASiS, patientjournal och andra system som hanterar patientuppgifter. Sekretessmarkering kan föreligga och då gäller ovanstående förmedlanderutiner.

Hantering av anställda med skyddade personuppgifter

Medarbetare som erhållit skyddade personuppgifter från Skatteverket ska informera närmaste chef eller motsvarande och visa upp ett beslut härom. Chefen får även informationen via Skånekatalogens systemförvaltning, som får uppgifterna från Skatteverket, att en medarbetare erhållit skyddade personuppgifter.

Medarbetare och chef ska ha en dialog om vilka behov eller begränsningar som medarbetarens situation kräver. Chef/motsvarande ansvarar för att lämna information om hur medarbetarens uppgifter visas i olika IT-system, hur det påverkar medarbetarens arbetsuppgifter och hur situationen kan lösas om personen inte kan fullgöra normala arbetsuppgifter. Omplacering kan bli nödvändig.

Anställda inom vård och omsorg finns registrerade i en gemensam katalog för vårdanställda i Sverige, Katalogtjänst HSA. Uppgifterna till HSA-katalogen hämtas från Skånekatalogen. Både HSA-katalogen och Skånekalogen är publika kataloger, där den anställdes arbetsplats- och yrkesuppgifter exponeras nationellt. Notera att HSA inte innehåller det som brukar betraktas som skyddsvärt, d.v.s. bild, hemadress och hemtelefonnummer. Men för personer med skyddade personuppgifter kan även annan information som t.ex. var man arbetar vara känsliga uppgifter som inte bör spridas.

För HSA-katalogen och Skånekatalogen är det standard att den som har skyddade personuppgifter inte visas vid sökningar och uppgifterna hanteras endast av ett fåtal katalogadministratörer. Den anställde måste göra ett aktivt ställningstagande om han eller hon vill vara synlig vid sökningar, och ansvarar då för de konsekvenser det kan medföra om uppgifterna exponeras. *Observera att ett synliggörande i HSA innebär att registrerad information om den anställde vid efterfrågan kan exporteras till alla HSA-anslutna tjänster som begär detta. Vidare erhåller dessa tjänster då ingen information om att den anställde har skyddade personuppgifter*.

Om den anställde arbetar i IT-system som är anslutna till HSA-katalogen eller Skånekatalogen blir uppgifterna synliga också i dessa. För en förteckning över vilka nationella e-tjänster som hämtar information om personer med skyddade personuppgifter hänvisas till www.inera.se/hsa under Dokument och Stödjande. https://www.inera.se/globalassets/tjanster/katalogtjanst-hsa/dokument/stodjande-dokument/tjanster_med_atkomst_till_skyddade_personuppgifter_fran_hsa.pdf

Om den anställde i sitt arbete utför aktiviteter i system som innehåller patientinformation loggas uppgifterna som användare i systemen oavsett om den anställde valt att synliggöra uppgifterna eller inte. Om patient begär loggutdrag från elektronisk journal i offentlig hälso- och sjukvård ska den anställde vara medveten om att arbetsgivaren måste lämna ut användaridentiteten.

Hos offentliga arbetsgivare gäller tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet, den så kallade offentlighetsprincipen. Principen garanterar var och en att fritt få ta del av allmänna handlingar som är offentliga och som finns hos en myndighet. På grund av offentlighetsprincipen ska personuppgifter i till exempel ett personregister hos en offentlig arbetsgivare lämnas ut till allmänheten i samma omfattning som traditionella handlingar. Det innebär att många uppgifter om arbetstagare kan bli tillgängliga för vem som helst om det inte råder sekretess enligt offentlighets- och sekretesslagen (t ex vid utlämnande av mailadresser).

I Region Skåne finns möjlighet till tre olika nivåer för hur den anställdes personuppgifter hanteras. Det är viktigt att chef tillsammans med anställd går igenom konsekvensen av respektive nivå med hänsyn till hotbild.

1) **Synlig:**
   I HSA-katalogen och Skånekatalogen är uppgifter synliga. Synkning sker mot Region Skånes REG-domän och mailsystem. Det innebär att den anställde får en personlig inloggning till Region Skånes datorer/nätverk och får tillgång till mail.

2) **Ej synlig, med personlig inloggning och mail:**
   I HSA-katalogen och Skånekatalogen är uppgifter inte synliga och uppgifterna hanteras endast av ett fåtal katalogadministratörer. Den anställde får personlig inloggning till Region Skånes datorer/nätverk och tillgång till mail. Mailadressen kommer inte att innehålla uppgifter om namn och kommer inte att vara synlig eller sökbar i mailsystemets adresskataloger.
   För att arbeta i system som hanterar patientuppgifter krävs personlig inloggning och den anställde lämnar också en logg varje gång han/hon varit aktiv i systemet. Om patient begär loggutdrag ska den anställde vara medveten om att Region Skåne måste lämna ut logguppgifter där den anställdes namn syns i enlighet med tryckfrihetsförordningens bestämmelser även om den anställde valt att uppgifterna inte ska vara synliga.

3) **Ej synlig, ingen personlig inloggning eller tillgång till mail:**
   I HSA-katalogen och Skånekatalogen hanteras uppgifterna på en skyddad gren av ett fåtal katalogadministratörer. Uppgifterna visas inte vid sökningar och de synkas inte till Region Skånes REG-domän och mailsystem. Det innebär att den anställde inte kan logga in på Region Skånes datorer och inte ha tillgång till mail.

Ställningstagande till publicering av personuppgifter i HSA, Skånekatalogen och andra IT-system ska göras av medarbetaren på blankett ”Ställnings-tagande till publicering av personuppgifter i HSA, Skånekatalogen och andra IT-system”. Personer med skyddade personuppgifter måste ge sitt ut-tryckliga tillstånd till om uppgifterna ska synliggöras eller inte. Ställnings-tagandet fyller medarbetaren i tillsammans med sin närmaste chef eller mot-svarande. Blanketten skickas med säker e-post till Skanekatalo-gen.systemforv@skane.se. Originalet bevaras/tillförs personalakten. Vid byte till annan tjänst inom Region Skåne ska nytt ställningstagande göras tillsammans med nya chefen. Vid avslutad anställning inom Region Skåne ska Skånekatalogens systemförvaltning meddelas via säker e-post.

För vägledning i specifika ärenden kan chef kontakta HR, förvaltningens ansvarige för Skånekakatalogen eller informationssäkerhetssamordnare.

Ordlista

HSA-katalogen	Katalogtjänst HSA är en elektronisk katalog som innehåller kvalitetsgranskade uppgifter om personer och verksamheter inom svensk vård och omsorg.
Skånekatalogen	Region Skånes elektroniska katalog som inne-håller uppgifter om samtliga medarbetare och verksamheter i Region Skåne och är tillgänglig för alla medarbetare via intranätet.
RSID	Varje medarbetares unika identitet i Skånekata-logen. RSID som används för bl.a. inloggning i Region Skånes nätverk.
REG-domän	Katalogtjänst som används för inloggning på Region Skånes datorer, servrar och många av systemen.

Bilaga 1

Information till dig som har skyddade personuppgifter och som arbetar inom Region Skåne

Om du erhållit skyddade personuppgifter från Skatteverket ska du informera närmaste chef eller motsvarande och visa upp ett beslut härom. Du och chefen ska ha en dialog om vilka behov eller begränsningar som din situation kräver.

Som anställd inom vård och omsorg finns du registrerad i en gemensam katalog för vårdanställda i Sverige, Katalogtjänst HSA. Uppgifterna om dig hämtas från Skånekatalogen.
Både HSA-katalogen och Skånekalogen är publika kataloger, där anställdas arbetsplats- och yrkesuppgifter exponeras nationellt. Notera att HSA inte innehåller det som brukar betraktas som skyddsvärt, d.v.s. bild, hemadress och hemtelefonnummer. Men för personer med skyddade personuppgifter kan även annan information som t.ex. var man arbetar vara känsliga uppgifter som inte bör spridas.

För HSA-katalogen och Skånekatalogen är det standard att den som har skyddade personuppgifter inte visas vid sökningar och uppgifterna hanteras endast av ett fåtal katalogadministratörer. Du måste göra ett aktivt ställningstagande om du vill att dina uppgifter ska vara synliga vid sökningar, och ansvarar då för de konsekvenser det kan medföra om uppgifterna exponeras. *Observera att ett synliggörande i HSA innebär att registrerad information om dig vid efterfrågan kan exporteras till alla HSA-anslutna tjänster som begär detta. Vidare erhåller dessa tjänster då ingen information om att du har skyddade personuppgifter.*

Om du arbetar i IT-system som är anslutna till HSA-katalogen eller Skånekatalogen blir dina uppgifter synliga också i dessa. För en förteckning över vilka nationella e-tjänster som hämtar information om personer med skyddade personuppgifter hänvisas till dokumentet ”Tjänster med åtkomst till personer med skyddade personuppgifter från HSA” på www.inera.se/hsa under Dokument och Stödjande.
https://www.inera.se/globalassets/tjanster/katalogtjanst-hsa/dokument/stodjande-dokument/tjanster_med_atkomst_till_skyddade_personuppgifter_fran_hsa.pdf

Om du i ditt arbete utför aktiviteter i system som innehåller patientinformation loggas dina uppgifter som användare i systemen oavsett om du valt att synliggöra dina uppgifter eller inte. Om patient begär loggutdrag från elektronisk journal i offentlig hälso- och sjukvård ska du vara medveten om att din arbetsgivare måste lämna ut din användaridentitet.

Hos offentliga arbetsgivare gäller tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet, den så kallade offentlighetsprincipen. Principen garanterar var och en att fritt få ta del av allmänna handlingar som

är offentliga och som finns hos en myndighet. På grund av offentlighetsprincipen ska personuppgifter i till exempel ett personregister hos en offentlig arbetsgivare lämnas ut till allmänheten i samma omfattning som traditionella handlingar. Det innebär att många uppgifter om arbetstagare kan bli tillgängliga för vem som helst om det inte råder sekretess enligt offentlighets- och sekretesslagen (t ex vid utlämnande av mailadresser).

I Region Skåne finns möjlighet till tre olika nivåer för hur dina personuppgifter som anställd hanteras. Det är viktigt att du tillsammans med din chef går igenom konsekvensen av respektive nivå med hänsyn till hotbild.

1) **Synlig:**
   I HSA-katalogen och Skånekatalogen är dina uppgifter synliga. Synkning sker mot Region Skånes REG-domän och mailsystem. Det innebär att du får en personlig inloggning till Region Skånes datorer/nätverk och får tillgång till mail.

2) **Ej synlig, med personlig inloggning och mail:**
   I HSA-katalogen och Skånekatalogen är dina uppgifter inte synliga och uppgifterna hanteras endast av ett fåtal katalogadministratörer. Du får personlig inloggning till Region Skånes datorer/nätverk och tillgång till mail. Mailadressen kommer inte att innehålla uppgifter om namn och kommer inte att vara synlig eller sökbar i mailsystemets adresskataloger.
   För att arbeta i system som hanterar patientuppgifter krävs personlig inloggning och den anställde lämnar också en logg varje gång han/hon varit aktiv i systemet. Om patient begär loggutdrag ska den anställde vara medveten om att Region Skåne måste lämna ut logguppgifter där den anställdes namn syns i enlighet med tryckfrihetsförordningens bestämmelser även om den anställde valt att uppgifterna inte ska vara synliga.

3) **Ej synlig, ingen personlig inloggning eller tillgång till mail:**
   I HSA-katalogen och Skånekatalogen hanteras dina uppgifter på en skyddad gren av ett fåtal katalogadministratörer. Dina uppgifter visas inte vid sökningar och de synkas inte till Region Skånes REG-domän och mailsystem. Det innebär att du inte kan logga in på Region Skånes datorer och inte ha tillgång till mail.

Ordlista

HSA-katalogen	Katalogtjänst HSA är en elektronisk katalog som innehåller kvalitetsgranskade uppgifter om personer och verksamheter inom svensk vård och omsorg.
Skånekatalogen	Region Skånes elektroniska katalog som innehåller uppgifter om samtliga medarbetare och verksamheter i Region Skåne och är tillgänglig för alla medarbetare via intranätet.
RSID	Varje medarbetares unika identitet i Skånekatalogen. RSID som används för bl.a. inloggning i Region Skånes nätverk.
REG-domän	Katalogtjänst som används för inloggning på Region Skånes datorer, servrar och många av systemen.

Ställningstagande till publicering av personuppgifter i HSA, Skånekatalogen och andra IT-system

Anställda med skyddade personuppgifter måste ge sitt uttryckliga tillstånd till om uppgifterna ska synliggöras eller inte. Ställningstagandet fylls i tillsammans med närmaste chef.

☐ Jag ger mitt tillstånd till att mina personuppgifter synliggörs både i HSA, Skånekatalogen och andra IT-system som används i Region Skåne.

☐ Jag vill inte att mina personuppgifter synliggörs i HSA, Skånekatalogen och andra IT-system som används i Region Skåne, men vill ha personlig inloggning till Region Skånes nätverk och tillgång till mail.

☐ Jag vill inte att mina personuppgifter synliggörs i HSA, Skånekatalogen och andra IT-system som används i Region Skåne. Jag får ingen personlig inloggning till Region Skånes nätverk och inte tillgång till mail.

Underskrifter
Som medarbetare med skyddade personuppgifter har jag tagit del av dokumentet ”Till dig som har skyddade personuppgifter och som arbetar i Region Skåne” och har valt att mina personuppgifter hanteras enligt ovan.

Ort och datum _____ Personnummer _____

Namnunderskrift _____ Namnförtydligande _____

Som ansvarig chef/motsvarande intygar jag att personen har tagit del av dokumentet ”Till dig som har skyddade personuppgifter och som arbetar i Region Skåne” och att dialog har skett inför ställningstagandet ovan.

Namnunderskrift _____ Namnförtydligande _____

RSID _____ Verksamhet/enhet _____

Blanketten skickas med säker e-post till Skanekatalogen.systemforv@skane.se