

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

BESLUT

Datum 2021-09-03
Dnr 2021-0000001

1 (10)

Instruktion för hantering av skyddade personuppgifter - anställda

Tidigare beslut om instruktion för hantering av skyddade personuppgifter har omfattat både patienter och anställda.

Regiondirektören har gett hälso- och sjukvårdsdirektören i uppdrag att fortsatt hantera och besluta om ny instruktion avseende hantering av patienter med skyddade personuppgifter.

Detta beslut avser anställda och innebär ingen förändring i hantering utan är en administrativ åtgärd till följd av uppdelningen.

Regiondirektören beslutar enligt bifogat underlag och att ” Instruktion för hantering av skyddade personuppgifter - anställda”, börjar gälla 2021-11-01.



Alf Jönsson
Regiondirektör

Instruktion för hantering av skyddade personuppgifter - anställda

Innehåll

Inledning	3
Bakgrund.....	3
Legala krav	3
Eget ansvar.....	4
Skatteverkets förmedlingsuppdrag/postförmedling.....	4
Ansvar.....	4
Hantering av anställda med skyddade personuppgifter	5
Termer, begrepp och definitioner	7
Bilaga 1	8
Bilaga 2.....	10

Inledning

Tidigare beslut om instruktion för hantering av skyddade personuppgifter har omfattat både patienter och anställda. Beslut "Instruktion för hantering av skyddade personuppgifter" 2019-11-08, dnr: 1800025 upphör att gälla 2021-11-01 och ersätts då av särskild instruktion för hantering av patienter. Denna instruktion avseende anställda innebär ingen förändring i hantering utan är en administrativ åtgärd till följd av uppdelningen.

Bakgrund

Uppgifter inom folkbokföringen 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, skyddad folkbokföring 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

Offentlighets- och sekretesslagen (OSL) (SFS 2009:400) reglerar användningen av "sekretessmarkering". Person som är utsatt för hot kan hos Skatteverket få en markering om sekretess (sekretessmarkering) i folkbokföringsregistret. En sekretessmarkering är den lägre graden av skyddade personuppgifter. Sekretessmarkering gäller under 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. Även person som genomgått könsbyte kan erhålla sekretessmarkering.

Folkbokföringslagen (SFS 1991:481) reglerar skyddet "skyddad folkbokföring". Skyddad folkbokföring tillgrips då sekretessmarkering inte ger tillräckligt skydd. Bostadsadress registreras inte i folkbokföringsdatabasen. En person med skyddad folkbokföring är i folkbokföringsregistret registrerad med sitt personnummer men på en särskild adress, s.k. förmedlingsuppdragsadress. Sekretessen är stark för personuppgifter för personer med skyddad folkbokföring. Dessa uppgifter måste därför hanteras ytterst noggrant och normalt sett inte lämnas ut. Det måste vara helt klarlagt att ett utlämnande kan göras utan någon risk för den hotade och förföljda personen. Skyddet beslutas av Skatteverket.

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. Region Skåne har ingen kännedom om skyddet och hanterar därmed patienten enligt normala rutiner.

Eget ansvar

Av Skatteverkets vägledning för hantering av skyddade personuppgifter i svensk förvaltning (2019) framkommer att en person som har skyddad folkbokföring eller sekretessmarkerade personuppgifter måste vara mycket noga med hur hen hanterar sina uppgifter. Till exempel behöver den som har skyddade personuppgifter själv kontrollera om en uppgift som lämnas till en myndighet blir sekretesskyddad hos myndigheten. Det framkommer också att det ligger ett ansvar på den enskilde att själv upplysa om skyddade personuppgifter eftersom det inte åligger en myndighet att utan anledning kontrollera om en person har sekretessmarkering i folkbokföringen. Det kan dock behöva konstateras vilket sekretesskydd personen har, för att dokumentation ska ske på rätt sätt. För att kontrollera om en person har skyddade personuppgifter kan man vända sig till Skatteverkets sekretessgrupp tel 010-5735500, vardagar 09:00-15:00. Läs mer om sekretesskydden på <https://www.skatteverket.se>

Skatteverkets förmedlingsuppdrag/postförmedling

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. Det brev som ska förmedlas ska läggas i ett innerkuvert med Region Skånes (alternativt privat vårdgivares) logotyp samt uppgift om avsändande förvaltning (alternativt sjukhus/vårdcentral) för att Skatteverket ska kunna returnera försändelsen om de inte kan nå mottagaren. Skriv personens personnummer och namn (om namnet är känt) på kuvertet. Lägg kuvertet i ett ytterkuvert och skriv Skatteverkets förmedlingsadress på det yttre kuvertet:

Skatteverkets förmedlingsuppdrag
Box 2820
403 20 Göteborg

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.

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

Ansvar

Verksamhetschef/motsvarande

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

Systemägarens ansvar

Systemägaren, genom systemansvarig, ska se till att IT-stöd kan hantera skyddade personuppgifter på ett säkert sätt. Region Skånes IT-system ska signalera för personal vilken typ av skydd en person har. För mer information, se respektive systems tillämpningsanvisningar.

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 Skånekatalogen 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 anställda måste göra ett aktivt ställningstagande om hen 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 anställda vid efterfrågan kan exporteras till alla HSA-an slutna tjänster som begär detta. Vidare erhåller dessa tjänster då ingen information om att den anställda har skyddade personuppgifter.

Om den anställda 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, se https://inera.atlassian.net/wiki/download/attachments/397772004/tjanster_med_atkomst_till_skyddade_personuppgifter_fran_hsa.pdf

Om den anställda i sitt arbete utför aktiviteter i system som innehåller patientinformation loggas uppgifterna som användare i systemen oavsett om den anställda valt att synliggöra uppgifterna eller inte. Om patient begär loggutdrag från elektronisk journal i offentlig hälso- och sjukvård ska den anställda 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 anställda 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 anställda 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 anställda lämnar också en logg varje gång han/hon varit aktiv i systemet. Om patient begär loggutdrag ska den anställda vara medveten om att Region Skåne måste lämna ut logguppgifter där den anställdes namn syns i enlighet med tryckfrihetsförordningens bestämmelser även om den anställda 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 anställda 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 ”Ställningstagande till publicering av personuppgifter i HSA, Skånekatalogen och andra IT-system”. Personer med skyddade personuppgifter måste ge sitt uttryckliga 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 Skanekatalogen.systemforv@skane.se Originalen 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 Skånekatalogen eller informationssäkerhetssamordnare.

Termer, begrepp och definitioner

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.

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 Skånekatalogen 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", se https://inera.atlassian.net/wiki/download/attachments/397772004/tjanster_med_atkomst_till_skyddade_personuppgifter_fran_hsa.pdf på Ineras hemsida.

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 logg-uppgifter 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.

Bilaga 2

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.

Ställningstagande

- 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