Beslutad av: Maria Fast, enhetschef säkerhet och beredskap 2021–11-24

Diarienummer: RS 2021–05924

Giltighet: från 2021-11-30 till 2026-11-30

Riktlinje verkställighet

Hantering när person har skyddade personuppgifter från Skatteverket

Riktlinjen gäller för: Samtliga förvaltningar och helägda bolag i Västra Götalandsregionen

Innehållsansvar: Koncernkontoret, Enheten säkerhet och beredskap

Dokumentet ersätter:
Rutin (RS 2019–05577) hantering av skyddade personuppgifter från Skatteverket

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Syfte och innehåll....3
Termer och begrepp....4
Ansvar för skyddade personuppgifter....4
Verksamhetschefens ansvar....4
Systemägarens ansvar....5
Eget ansvar....5
Definitioner skyddade personuppgifter....5
Sekretessmarkering....6
Skyddad folkbokföring....6
Fingerade personuppgifter....6
Krav på identifiering av person med skyddade personuppgifter....6
Patient med skyddade personuppgifter....7
Koppling av reservidentitet till personnummer med skyddsmarkering....7
Medarbetare med skyddade personuppgifter....7
IT-anpassningar för medarbetare med skyddsmarkerade personuppgifter....7
IT-system....8
Post till personer med skyddade personuppgifter....9
Mer information....9

Syfte och innehåll

Uppgifter som registreras i folkbokföringen är som huvudregel offentliga. I vissa fall kan det dock skada en person om uppgifter lämnas ut. En person som är utsatt för hot eller annan allvarlig brottslighet kan, efter beslut av Skatteverket, få skyddade personuppgifter.

I Västra Götalandsregionen (VGR) ska skyddade personuppgifter hanteras med mycket stor försiktighet för att öka tryggheten och ge skydd åt de personer som lever i rädsla på grund av att de riskerar att utsättas för brott. Syftet är att förhindra att obehöriga ska kunna ta del av skyddade personuppgifter vilket kan innebära risk för liv och hälsa.

Denna riktlinje anger ett ramverk för utformning och styrning av administration och IT-system för att förhindra att skyddsvärda uppgifter om personer med skyddade personuppgifter lämnas ut till obehöriga.

Personuppgifter som avses i riktlinjen gäller för medarbetare, patienter, elever eller andra vars personuppgifter hanteras av VGR.

Riktlinjen utgår ifrån VGRs policy för säkerhet och beredskap (RS 2018–00129)[1] samt riktlinje för verksamhetsskydd (RS 2018–00129)[2] och riktlinje för informationssäkerhet (RS 2018–00129)[3].

Riktlinjen gäller för alla VGR:s förvaltningar, majoritetsägda bolag, privata vårdgivare med vårdavtal samt avtalsparter där det i avtalet anges att regionens regelverk ska följas.

Utifrån denna riktlinje kan systemspecifika och verksamhetsanpassade rutiner och anvisningar tas fram.

[1] VGRs policy för säkerhet och beredskap (RS 2018–00129)
[2] Riktlinje för verksamhetsskydd (RS 2018–00129)
[3] Riktlinje för informationssäkerhet (RS 2018–00129).

Termer och begrepp

Begrepp	Innebörd
Personuppgiftstjänst	Tjänst som hanterar personuppgifter.
Reservidentitet	Samlingsbegrepp för lokal reservidentitet och nationell reservidentitet.[4]
Riskbedömning	Riskbedömning innebär att identifiera vilka skyddsvärda uppgifter som hanteras samt sannolikheten och konsekvensen om dessa skyddsvärda uppgifter lämnas ut till obehörig person.
Skadeprövning	Skadeprövningen görs för att kunna ta ställning till om den eller det som sekretessen ska skydda kan lida skada eller men om uppgiften eller handlingen lämnas ut.[5]
Skyddade personuppgifter	Samlingsbegrepp för personer som är utsatta för ett allvarligt och konkret hot och efter ansökan hos Skatteverket har fått skyddade personuppgifter. Det finns tre typer av skyddade personuppgifter: sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter.
Skyddsmarkering	Samlingsbegrepp för de markeringar som Skatteverket anger på personer med Sekretessmarkering och skyddad folkbokföring. Fingerade personuppgifter kommer inte med skyddsmarkering till våra system.
Skyddsvärda uppgifter	Information eller uppgifter som kan avslöja var person med skyddade personuppgifter arbetar, bor, befinner sig tillfälligt samt uppgifter som gör det möjligt att kartlägga personen.

Ansvar för skyddade personuppgifter

Förvaltningschef eller vd ansvarar för att regionala riktlinjer, rutiner och arbetssätt efterföljs.

Verksamhetschefens ansvar

Verksamhetschef ansvarar för att regionala riktlinjer, rutiner och arbetssätt är kända inom verksamheten och att medarbetarna har fått den utbildning och information som behövs för

[4] Sök efter, registrera och koppla ihop reservnummer - Vårdgivarwebben Västra Götalandsregionen (vgregion.se)
[5] Hur fungerar en sekretessbestämmelse? | Rättslig vägledning | Skatteverket

att kunna följa dessa regler. Verksamhetschef ansvarar för att det finns lokala anpassningar för hantering av personer med skyddsmarkerade personuppgifter där behov finns.

Systemägarens ansvar

Systemägaren ansvarar för att IT-systemen kan hantera skyddade personuppgifter på ett säkert sätt samt att IT-system tydligt ska visa för användaren att en person har skyddade personuppgifter.

Eget ansvar

Personer med skyddade personuppgifter har även ett egenansvar att skydda uppgifter om sig själv som anses vara skyddsvärda.

Definitioner skyddade personuppgifter

Skyddade personuppgifter är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna inom folkbokföringen. Den som är utsatt för hot eller annan allvarlig brottslighet kan i vissa fall få skyddade personuppgifter. Skatteverket beslutar efter ansökan om att utsatt person och ibland även anhöriga ska ha en skyddande markering i folkbokföringsregistret. En person kan inte åberopa skyddad identitet utan beslut från Skatteverket.

Huvudregeln för skyddade personuppgifter i VGR är att samtliga skyddsvärda uppgifter ska skyddas med sekretess och ej vara sökbara internt eller externt. Vad som är skyddsvärt kan variera beroende på hotbild. Adress är i regel den uppgift som är mest skyddsvärd, men även andra uppgifter inom folkbokföringen kan behöva skyddas, till exempel uppgifter om anhöriga och uppgifter som kan röja var personen eller dennes anhöriga kan befinna sig.

Skyddade personuppgifter har tre sekretessnivåer:

1. Sekretessmarkering
2. Skyddad folkbokföring
3. Fingerade personuppgifter.

IT-systemen ska endast visa personnummer tillsammans med texten ”Skyddad uppgift” i namnfälten samt adressen till Skatteverkets förmedlingsuppdrag. Systemägare ska tillse att IT-system kan hantera skyddade personuppgifter efter satta skyddsåtgärder, administration och behandling av skyddade personuppgifter ska ske säkert för att för att undvika att skyddade personuppgifter röjs. Risken för att skyddade personuppgifter lämnas ut, av misstag eller medvetet ökar med antalet handläggare som kan ta del av skyddade personuppgifter. Administration och system ska utformas så att endast ett fåtal personer med särskild behörighet har tillgång till uppgifterna. Individuella undantag kan vara möjliga eftersom utsattheten och vad som betraktas som skyddsvärda uppgifter kan variera från individ och situation. Bedöms vissa uppgifter som ej skyddsvärda kan individuella undantag göras efter dokumenterat samråd och samtycke. Undantag kan göras först efter en riskbedömning.

Sekretessmarkering

Sekretessmarkering är den lägre graden av skyddade personuppgifter och den vanligaste typen av skydd. Om det föreligger särskild anledning att en person eller någon närstående, kan lida skada eller men om uppgifter om person lämnas ut så kan Skatteverket efter ansökan från person, bedöma om person ska skyddas i folkbokföringsregistret med en sekretessmarkering.

Markeringen omfattar alla uppgifter om en person. Omprövning av sekretessmarkering sker i regel efter två år.

Skyddad folkbokföring

När hotbilden mot en person är mycket stark kan personen få skyddad folkbokföring enligt 16 § folkbokföringslagen.[6] En markering för skyddad folkbokföring registreras då i folkbokföringsdatabasen. Personen är folkbokförd på en annan folkbokföringsort än där personen är bosatt.

Skyddad folkbokföring är ett starkare skydd som innebär att personen vanligtvis behöver flytta till en ny bostad och byta arbetsplats för att skyddet ska fungera. Fördelen med skyddad folkbokföring är att den verkliga bostadsadressen inte framgår av folkbokföringsregistret och därmed inte heller sprids till aviseringsmottagarna. Den gamla adressen tas bort och personen registreras på Skatteverkets särskilda adress.

Fingerade personuppgifter

Vid särskilt allvarliga hot kan en person medges att använda annan identitet. Det innebär att personen får ett nytt personnummer. Den registreras på ett sådant sätt att det inte framgår att det rör sig om fingerade personuppgifter. Ansökan om fingerade personuppgifter görs hos polisen. Om verksamheten i VGR av någon anledning får kännedom om att en person har fått en identitet med fingerade personuppgifter är det av största vikt att den informationen inte röjs och att identiteten inte kopplas samman med tidigare identitet.

Krav på identifiering av person med skyddade personuppgifter

Krav på identitetskontroll gäller även för personer som har skyddade personuppgifter.

Patientdatalagen[7] och Socialstyrelsens författning om journalföring och behandling av personuppgifter i hälso- och sjukvården[8] ställer krav på unik identifiering av både patienter och medarbetare i vårdgivarnas informationssystem.

[6] Folkbokföringslag (1991:481) Svensk författningssamling 1991:1991:481 t.o.m. SFS 2021:375 - Riksdagen
[7] Patientdatalag (2008:355) Svensk författningssamling 2008:2008:355 t.o.m. SFS 2021:365 - Riksdagen
[8] Senaste version av HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården - Socialstyrelsen

Att uppge annans identitet är straffbart enligt BrB 4 kap. 6 b § (olovlig identitetsanvändning)[9] och ska polisanmälas

Patient med skyddade personuppgifter

Att fastställa varje patients identitet är en fråga om patient- och informationssäkerhet och handlar dels om att journal ska föras på rätt patient och att ha tillgång till korrekt information om patient. Detta för att kunna ge relevant vård, undvika olovlig identitetsanvändning och kunna ge det skydd som krävs vid skyddade personuppgifter.

Alla människor har rätt till akut bedömning och vård och ingen kan nekas akut vård på grund av att denne saknar legitimation, ovilja eller oförmåga att uppge sin identitet. Om en patient inte kan, och i vissa fall inte vill, styrka sin identitet och ändå ska få vård ska personen upplysas om att reservidentitet kommer att tilldelas och att journalföring kommer att ske med denna reservidentitet. En reservidentitet kan medföra begränsningar i vården.

Koppling av reservidentitet till personnummer med skyddsmarkering

Verksamheter som använder reservidentitet ansvarar för att bevaka och sammankoppla reservidentitet med personnummer så snart det är möjligt. Sammankoppling till ett personnummer som har skyddsmarkering ska föregås av en riskbedömning, då koppling sker i personuppgiftstjänster och journalsystem där information delas regionalt och nationellt.

För information gällande reservnummer se rutin för regionalreservnummer hantering inom VGR[10] samt vårdgivarwebbens[11] information om att registrera och koppla reservnummer.

Medarbetare med skyddade personuppgifter

Huvudregeln i VGR är att medarbetare med skyddade personuppgifter inte ska vara offentligt eller internt sökbara. Skyddsvärda uppgifter ska behandlas med sekretess. Ansvarig chef ska tillsammans med medarbetare som fått beslut om skyddade personuppgifter göra en gemensam riskbedömning samt kartlägga vilken information som visas i regionens IT-systemen och därefter tillse att skyddsvärd information skyddas.

IT-anpassningar för medarbetare med skyddsmarkerade personuppgifter

I elektroniska patientinformationssystem, loggas personuppgifter och kan då utgöra en risk för att skyddsvärda uppgifter röjs. Hotbild och åtgärder för skydd avgör begränsningar och

[9] Brottsbalk (1962:700) Svensk författningssamling 1962:1962:700 t.o.m. SFS 2021:397 - Riksdagen
[10] Rutin för regional reservnummerhantering inom VGR (vgregion.se)
[11] Sök efter, registrera och koppla ihop reservnummer - Vårdgivarwebben Västra Götalandsregionen (vgregion.se)

möjligheten att utföra vissa arbetsuppgifter. Riskbedömningen ligger till grund för utformning av individuella och anpassade skyddsåtgärder. Individuella anpassningar är möjliga efter medarbetarens skriftliga samtycke. Skyddsåtgärder kan komma i konflikt med sjukvårdens krav på spårbarhet som i vissa fall kan kräva att medarbetare med stort behov av skydd inte kan utföra de arbetsuppgifter tjänsten kräver. Är hotbilden och skyddsbehov särskilt stark och anpassningar inte lämpliga kan omplacering bli nödvändig.

Att ta med vid riskbedömningen:

- Beskriv hotbild, sannolikhet och konsekvens för medarbetaren och arbetsplatsen.
- Var och hur är medarbetaren sökbar och internt och offentligt?
- Vilka ska informeras om att medarbetaren har skyddade personuppgifter? Chefer, arbetskamrater?
- Hur ska chefer och medarbetare förhålla sig till frågor från andra som rör medarbetaren?
- Vad händer och vilka åtgärder ska vidtas om skyddade personuppgifter lämnas ut av misstag? Hur kan skadan minimeras?

IT-system

Systemägaren ska tillse att deras IT-system kan hantera skyddade personuppgifter och att det finns koppling mellan IT-system och av VGR vald personuppgiftstjänst.

IT-system ska:

- Tydligt påvisa skyddade personuppgifter.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
- Vid utveckling av IT-stöd ska behandlingen av skyddade personuppgifter särskilt beaktas.
- Ha system för loggkontroll som möjliggör kontroll av vilka som har tagit del av skyddade personuppgifter.

Huvudregeln för personer med skyddade personuppgifter är att VGR:s IT-system tydligt visar att en person har skyddade personuppgifter. Samtliga personuppgifter behandlas som skyddsvärda tills en riskbedömning genomförts. Om ett personnummer med skyddsmarkering har kopplade personidentiteter hanteras även dessa som skyddsmarkerade, dvs personuppgifterna som finns registrerade skall hanteras på likvärdigt sätt som personnumret.

En person med skyddade personuppgifter bör enbart kunna hanteras i ett system då fullständigt personnummer är känt, delar av personnummer och personuppgifter bör ej vara sökbara internt eller externt. IT-systemen ska endast visa personnummer tillsammans med texten ”Skyddad uppgift” i namnfälten samt adressen till Skatteverkets förmedlingsuppdrag. Systemen ska agera på skyddsmarkering så att posthantering sker

enligt Skatteverkets rutin[12] ”skicka post till någon med skyddade personuppgifter”. Avregistreringsorsak, kön och födelsedatum kan visas om verksamheten har behov av det.

Individuella undantag kan göras efter samråd med person och om det är möjligt att hantera i IT-systemet. Dokumentera alltid individuella undantag i samråd med personen. Pappersbaserad information ska förvaras i separat låst utrymme, dit endast behörig personal har tillträde.

Utifrån denna riktlinje kan lokala verksamhetsanpassade anvisningar eller rutiner tas fram för att anpassas efter verksamhetens behov, system och förutsättningar.

Externa aktörer och privata vårdgivare i vårdavtal kopplade till VGR ansvarar för att säkerställa att skyddade personuppgifter behandlas enligt denna rriktlinje samt att använda system som synkroniserar med VGR samt nationella personuppgiftstjänster och system.

Post till personer med skyddade personuppgifter

Skicka post till någon med skyddade personuppgifter – Skatteverkets förmedlingsuppdrag | Skatteverket

Mer information

Tjänster med åtkomst till skyddade personuppgifter från HSA.pdf

Skyddade personuppgifter | Skatteverket

Hur fungerar en sekretessbestämmelse? | Rättslig vägledning | Skatteverket

Sök efter, registrera och koppla ihop reservnummer - Vårdgivarwebben Västra Götalandsregionen (vgregion.se)

Rutin för regional reservnummerhantering inom VGR (vgregion.se)

[12] Skicka post till någon med skyddade personuppgifter – Skatteverkets förmedlingsuppdrag | Skatteverket