# Personuppgifter på intyg

Utredning av dataskyddsperspektivet

## Ändringshistorik

| Datum | Revision | Beskrivning | Författare |
|---|---|---|---|
| 2018-06-12 | 1 | Första version | Christian Hilmersson |
| 2018-06-25 | 2 | Uppdaterad med hänsyn till input från/dialog med Peter H.<br>La till bildtext samt resonemang kring force majeure. | Christian Hilmersson |
| 2018-06-26 | 3 | Ytterligare uppdateringar i bild och bildtext | Christian Hilmersson |
| 2018-06-26 | 4 | La till person-id i bild | Christian Hilmersson |
| 2018-06-26 | 5 | Bytt dokumentrubrik samt ändrat till personnummer i bild | Christian Hilmersson |
| 2018-06-27 | 6 | Uppdaterat efter avstämning med Manolis Nymark | Christian Hilmersson |
| 2018-06-27 | 7 | Uppdaterat dokumentmall samt adderat text om bakgrund | Lena Furubacke |

# Innehållsförteckning

# 1 Bakgrund

Projektet Intygstjänster fick 2014 en förfrågan från Stockholms läns landsting om det var möjligt att tillåta intygsutfärdande för personer med skyddade personuppgifter då det var ett problem att hantera dessa analogt (på pappersblanketter). Projektet startade därför 2014 en utredning om detta 2014 i dialog med Socialstyrelsen och andra landsting. Man identifierade tidigt ett Moment-22 läge om namn och adress lagras i intyget i Intygstjänsten och personen senare förses med skyddade personuppgifter. Intygstjänster kan då inte exkludera information i den signerade filen, för då bryts signeringen. Styrgruppen förordade därför en lösning där Intygstjänsten ALDRIG lagrar namn och adress i intyg som tillåts utfärdas elektroniskt för personer med skyddad identitet.

Socialstyrelsen uppdaterade 2015 intygsföreskriften och gjorde det då möjligt att ansöka om undantag till intygsföreskriften (SOSFS 2005:29) from 1 juni 2015. Inera skickade 2015-08-11 in en ansökan på uppdrag av landstingen om undantag att lagra namn- och adressuppgifter på Försäkringskassans intyg för att möjliggöra elektroniskt intygsutfärdande för personer med skyddad identitet. Socialstyrelsens svar inkom 2015-11-20 och vi beviljades undantag från att lagra namn och adress på Försäkringskassans intyg och därmed möjliggöra att dessa intyg kan utfärdas även för personer med skyddade personuppgifter.

Ärendet har utretts av Inera i samråd med Socialstyrelsen, Försäkringskassan och landsting och sedermera implementerats samt gemensamt testats och införlivats i tjänsterna. Lösningen har resulterat i verksamhetsregler och påverkar tjänsterna Webcert, Mina intyg, Intygstjänsten och Rehabstöd. Stödet för att hantera intyg för personer med skyddad identitet för Försäkringskassans nya intyg produktionssattes i Webcert (version 5.3) 21 november 2017 och har idag driftsatts av 9 landsting som valt att göra integration med Webcert från sina journalsystem, ytterligare 9 landsting kommer driftsätta denna lösning under hösten 2018.

## 1.1 Syfte

Dokumentets syfte är att belysa de frågeställningar som i efterhand uppkommit i ärendet kring lagring av namn och adressuppgifter samt försöka ge en helhetsbild ur ett högnivåperspektiv för att sprida förståelse som kan ligga till grund för en konstruktiv dialog.

# 2. Behov

Socialstyrelsens intygsföreskrift anger att det i ett medicinskt underlag skall ingå namn och adress för den invånare intyget avser.

I ett system som baseras på manuell hantering av pappersintyg är ett sådant krav rimligt då det finns externa faktorer som påverkar datakvaliteten. Det kan till exempel röra sig om trasiga eller skrynkliga papper som blir svårlästa, dessa kan även ha scannats med resultat att vissa uppgifter blir oläsliga Det kan även relatera till den mänskliga faktorn i form av felskrivningar, felläsningar, svårtydd handstil med mera.

På grund av risken för mänskliga fel, att man till exempel läser fel på personnummer, kan det således vara rimligt att det i de gränssnitt för hantering av intyg där intyg skall hanteras av en människa framgår både namn och personnummer.

Situationer då det tydligt bör framgå namn och personnummer i gränssnittet kan till exempel vara då en läkare skriver och signerar ett intyg eller då en handläggare hos Försäkringskassan handlägger ett ärende som innehåller ett intyg.

# 3. Krav

Utöver de funktionella krav som finns på ett system för delning av intygsdata mellan myndigheter finns även ett antal externa krav så som lagar, förordningar och föreskrifter.

Två källor för externa krav i processen med delning av intygsdata mellan myndigheter är dataskyddsförordningen (GDPR) samt Socialstyrelsens intygsföreskrift nedan.

Kärnan av den juridiska kravställningen kommer från dataskyddsförordningens (GDPRs) krav på uppgiftsminimering och inbyggt dataskydd (”privacy by design”) och dataskydd som standard (”privacy by default”). Intygstjänsterna har anpassats för att möjliggöra att intyg kan utfärdas för individer som har eller kan komma att få sekretessmarkering. Det har gjorts genom uppgiftsminimering, vilket också krävs av GDPR.

## 3.1 Praxis kring dataskydd

### 3.1.1 Vårdens tolkning

Som personuppgiftsansvarig har respektive vårdgivare ansvar för att invånarens personuppgifter skyddas i enlighet med dataskyddsförordningen.

Bedömningen är att för att kunna behandla personuppgifter krävs det bland annat att uppgifterna är nödvändiga för att utföra sina uppgifter, att det finns ett tydligt ändamål med behandlingen, att syftet till varför behandlingen är nödvändig går att beskriva, att man aldrig behandlar mer personuppgifter än vad som behövs.

Kan man inte uppfylla dessa punkter så är bedömningen att man inte lever upp till dataskyddsförordningen.

### 3.1.2 Utdrag från Datainspektionen

Nedan följer några utdrag från Datainspektionens webbsida ”Personuppgiftsbehandling hos myndigheter” (2018-06-12, https://www.datainspektionen.se/vagledningar/for-myndigheter/) angående dataskydd vid myndigheters behandling av personuppgifter. I ärendet intressanta delar har understrukits och fetmarkerats. Se länken ovan för fullständig formulering och kontext.

> *”**Vid behandling av personuppgifter måste myndigheter följa flera regelverk**:*
>
> - *dataskyddsförordningen (GDPR)*
> - *särskild registerförfattning*
> - *den kompletterande dataskyddslagen, det vill säga lagen med kompletterande bestämmelser till EU:s dataskyddsförordning”*

**Utdrag ur sektion Rättsliga grunder som myndigheter kan använda:**

> *” Personuppgifter får behandlas om det är nödvändigt för att uppfylla en rättslig förpliktelse. Den rättsliga förpliktelsen ska åligga den personuppgiftsansvarige och följa av EU-rätt eller svensk rätt.*
>
> *Behandling av personuppgifter är dessutom tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse. Uppgiften ska vara fastställd i EU-rätt eller svensk rätt, vilket innebär att den måste följa av det regelverk som gäller för myndighetens verksamhet.* ***Den behandling av personuppgifter som är nödvändig för att myndigheten ska kunna utföra dessa uppgifter kan då ske*** *med stöd av den rättsliga grunden uppgift av allmänt intresse.”*

**Utdrag ur *Rättsliga grunder med begräsning för myndigheter*:**

> *”En av de rättsliga grunderna är att behandlingen är nödvändig för ett berättigat intresse och att den registrerades intresse av skydd för sina personuppgifter inte väger tyngre, det vill säga vid en intresseavvägning.* ***Myndigheter kan emellertid inte stödja sin behandling på en intresseavvägning när de behandlar personuppgifter*** *som ett led i fullgörande av sina uppgifter.”*

Utöver dessa särskilda skrivelser för myndigheter följer här utdrag som sammanfattar det grundläggande principerna i dataskyddsförodningen 20168-06-12, https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

> ***Principerna innebär bland annat att ni som personuppgiftsansvariga***
>
> - *måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter*
> - *bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål*
> - ***inte ska behandla fler personuppgifter än vad som behövs för ändamålen***
> - ***ska se till att personuppgifterna är korrekta***
> - *ska radera personuppgifterna när de inte längre behövs*
> - *ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs*
> - ***ska kunna visa att och hur ni lever upp till dataskyddsförordningen.***

**Utdrag från sektion Nyhet: Ansvarsskyldighet**

> *En nyhet är dock att det inte längre är tillräckligt att följa lagen, utan* ***den som är ansvarig för personuppgiftsbehandlingen måste också kunna visa att och hur man följer bestämmelserna i dataskyddsförordningen****.*

**Utdrag ur sektion Ändamålsbegränsning**

> *”**Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga**. Det är till exempel inte tillräckligt att ange "kontroller" som ändamål för loggning och övervakning, utan att **också ange syftet** med kontrollen.”*

**Utdrag ur sektion Dokumentera ändamålen**

> *”Dokumentera vilka ändamål ni har med personuppgiftsbehandlingen. Det behöver ni för att kunna visa att ni uppfyller principen om ansvarsskyldighet.”*

**Utdrag ur sektion Personuppgifter som hör till saken**

> *”Ni ska aldrig behandla fler personuppgifter än vad som behövs, och de personuppgifter som behandlas ska vara tydligt kopplade till ändamålet. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, för att de kan vara "bra att ha".”*

## 3.2 Socialstyrelsens intygsföreskrift

### *Krav på innehåll i intyg enligt 10 kap 6 §* SOSFS 2005:29

*Enligt 10 kap 6 § SOSFS 2005:29 ska intyg som utfärdas inom hälso- och sjukvården innehålla följande uppgifter:*

1. *ändamålet med intyget,*
2. *intygspersonens namn, personnummer och adress,*
3. *hur identiteten styrkts,*
4. *intygsutfärdarens namn, kompetens och tjänsteställning eller befattning, och*
5. *intygsutfärdarens tjänsteställe eller mottagningslokal, adress och telefonnummer.*

#### 3.2.1 Ineras ansökan om undantag från Socialstyrelsens föreskrift

Socialstyrelsen justerade intygsföreskriften och gjorde det möjligt att ansöka om undantag till intygsföreskriften (SOSFS 2005:29) from 1 juni 2015.

Inera skickade 2015-08-11 in en ansökan på uppdrag av landstingen om undantag att lagra namn- och adressuppgifter på intyg för att möjliggöra elektroniskt intygsutfärdande för personer med skyddad identitet, se utdrag ur Ineras ”Ansökan om undantag enligt 10 kap 10 § SOSFS 2005:29” nedan:

## Intyg i Intygstjänsten

*Intyg i Intygstjänsten innehåller uppgifter i enlighet med kraven i Socialstyrelsens föreskrifter och således patientens namn och adress. Inera har tillsammans med representanter från hälso- och sjukvården identifierat att detta utgör ett problem när det gäller intyg för patienter med*

*sekretessmarkerade personuppgifter. Dessa personer har ett ökat behov av skydd och det är av yttersta vikt att deras personuppgifter inte röjs.*

*För att minimera risken för att sådana patienters identitet röjs bör elektroniska intyg inte innehålla fler personuppgifter än nödvändigt och därför endast upprättas elektroniskt om de kan sparas utan patientens namn och adress. För att detta ska vara möjligt i Intygstjänsten krävs ett undantag från kraven i 10 kap 6 § p. 2 SOSFS 2005:29. Då även historiska uppgifter om namn och adress kan vara känslig information för det fall en person får sekretessmarkerade personuppgifter, bör undantaget omfatta samtliga intyg i Intygstjänsten.*

### 3.2.2 Socialstyrelsens svar om undantag från Socialstyrelsens föreskrift

Socialstyrelsens svar på Ineras ansökan inkom till Inera 2015-11-20, se utdrag nedan

*Socialstyrelsens bedömning*

Föreskrifterna är utformade för att säkerställa att alla intyg inom hälso- och sjukvården innehåller nödvändiga uppgifter för att man på ett säkert sätt ska kunna identifiera vilken person intyget avser. Den aktuella intygstjänsten som Inera AB erbjuder vårdgivarna förmedlar elektroniska intyg. Inera AB uppger att det, för att vårdgivaren på ett säkert sätt ska kunna identifiera vilken person som avses med intyget som förmedlas genom tjänsten, är tillräckligt att det finns uppgifter om intygspersonens personnummer. Det finns inget behov av uppgift om namn och adress. Därutöver anför Inera AB att ett undantag från kravet på att alla intyg utöver personnummer även ska innehålla uppgifter om namn och adress är nödvändig för att vårdgivarna inom intygstjänsten ska kunna erbjuda skydd för personer med sekretessmarkerade personuppgifter.

Utifrån att det är en viktig princip vid all behandling av personuppgifter att inte behandla fler uppgifter än nödvändigt och mot bakgrund av det som anförts ovan anser Socialstyrelsen att det finns särskilda skäl att bifalla ansökan.

Beslut i detta ärende har fattats av generaldirektören Olivia Wigzell. I den slutliga handläggningen har avdelningschefen Erik Höglund och enhetschefen Georg Lagerberg deltagit. Juristen Maria Jacobsson har varit föredragande.

*Hos Socialstyrelsen pågår ett arbete med att ”Utreda och där det är möjligt anpassa intygsföreskriften hos Socialstyrelsen så att den understödjer en digital intygshantering på ett effektivt sätt.”*

# 4. Möjligheter och lösningsarkitektur

## 4.1 Datakvalitet vid elektronisk lagring

I ett system för elektronisk lagring av data bunden till en person finns inte samma risker för sammanblandning av information som återfinns vid manuell hantering. När läkaren har verifierat att namn och personnummer stämmer, signerat och sedan sparat ett intyg bundet till det angivna personnumret finns det ingen risk att lagringssystemet förvanskar eller misstolkar personnumret.

Den lagrade informationen kan sedan skickas vidare för att i de gränssnitt där så behövs kompletteras med personuppgifter. En sådan gränsyta kan t.ex. vara i Försäkringskassans handläggarvy.

## 4.2 Arkitekturella policys

Här beskrivs några av de grundläggande arkitekturella policys som ligger till grund för hur lösningen har utformats. Beskrivningen skall generellt ses i ljuset av behandling av personuppgifter men även specifikt i förhållande till möjlig sekretessmarkering av intygspersoner.

### 4.2.1 Undvik starka beroenden genom inkapsling

Det är ur ett tekniskt och arkitekturellt perspektiv en god idé att försöka gruppera system i delar på ett sätt som ger hög inkapsling och sammanhållning mellan data och funktionalitet inom respektive modul. Man strävar också efter att man mellan dessa moduler får en så låg grad av koppling till varandra som möjligt. Man vill så långt det går separera data och ansvarsområden i moduler som inte har påverkan på varandra.

Inte minst är detta viktigt då man designar stora och komplexa system med många inblandade parter och komponenter.

Genom att dela upp ett system i tydliga ansvarsområden utan onödiga beroenden sinsemellan blir det enklare att underhålla och överblicka enskilda delar av systemet. Förändringar i enskilda delar påverkar då i låg utsträckning andra delar av systemet.

Med andra ord, för att få så stor frihetsgrad som möjligt i systemets alla delar så strävar man efter att få en så låg grad av koppling mellan dem som möjligt.

I det här fallet handlar det om att hantera data som rör ett medicinskt intygande skiljt från data som rör person. Personuppgifter (som namn, adress och sekretessmarkering) har inte någon väsentlig koppling till innehållet i ett medicinskt intygande. Det medicinska intygandet (personens hälsotillstånd/historik) förändras inte i händelse av att personuppgifterna förändras, t.ex. genom sekretessmarkering av en person. Man vill därför undvika en stark koppling mellan dessa två datamängder.

Eftersom personuppgifter och innehållet i ett medicinskt intygande inte har någon naturlig koppling i sin funktion eller sitt tillstånd, bör de således kunna uppdateras oberoende av och utan påverkan på varandra.

Att med digital signatur hårt låsa fast vid tillfället aktuella personuppgifter till intygsdata får konsekvenser som exemplifierar problem som kan uppstå vid hög grad av koppling mellan olika

delar i ett system. En konsekvens av detta är att man vid sekretessmarkering av en person inte längre kan distribuera intyg som finns utfärdade på personen om de innehåller data som skall skyddas av sekretess så som namn. Detta trots att den medicinska informationen i intyget fortfarande är gällande och inte påverkas av en sekretessmarkering. Det är även tveksamt om man skulle kunna utfärda intyg på personer som redan har sekretessmarkering då dessa skulle tydligt skulle pekas ut genom avsaknad av namn på intyget. Man kan inte heller lägga tillbaka namn då sekretessmarkeringen tas bort.

Ytterligare en konsekvens blir således att vården i ett sådant läge behöver ansvara för implementation av unika policyer för sekretesshantering och personuppgiftshantering för respektive intygsmottagare, kanske skulle det sträcka sig så långt att läkaren behöver signera dubbla uppsättningar med intyg. Ett med personuppgifter och ett utan. Det kan i förlängningen röra sig om många policyer som skall hanteras och underhållas och man får då en hög grad av beroende mellan systemets delar (hög kopplingsgrad). Då en intygsmottagare i ett sådant scenario önskar ändra i sin policy måste intygsinfrastrukturen uppdateras med allt vad det innebär av synkronisering mellan integrerande parter, testning, release etc. Det är då enklare och mer kostnadseffektivt att respektive mottagare hanterar implementation av sin egen sekretesspolicy och vården hanterar den del som handlar om det medicinska intyget.

Genom att utelämna namn och adressuppgifter i intygsdata och endast binda intygsdata till personnummer löser man således problematik med att olika intygsmottagare kan ha olika rutiner för hur man bör/skall hantera sekretessmarkering. Det möjliggör därmed för varje intygsmottagare att implementera sin egen policy för hur de hanterar sekretess.

Man slipper man även problematik med att namn och adressuppgifter riskerar att vara utdaterade då en invånare har bytt namn och/eller flyttat.

Sist men inte minst förhåller man sig även till dataskyddsförordningen förbud mot att inte behandla mer personuppgifter än vad som krävs för att lösa uppgiften.

### 4.2.2 Inbyggt dataskydd och dataskydd som standard (Privacy by design & Privacy by default)

Att designa med inbyggt dataskydd betyder i korthet att systemet skall utformas på ett sätt så att lagring av personuppgifter minimeras. Det kan t.ex. ske genom att byta ut personuppgifter mot en pseudonym/nyckel. Att lagra person-id (t.ex. personnummer) som används som nyckel till andra personuppgifter kan sägas vara en typ av pseudonymisering. Man kan resonera kring om personnummer är en tillräckligt anonym pseudonym. Det är dock den nyckel som det idag finns inbyggt stöd för nationellt och i näst intill all befintlig infrastruktur och därmed den enda som är praktiskt tillämpningsbar över myndighetsgränser för tillfället.

Pseudonymiseringen innebär att intygsmottagare behöver hämta de uppgifter de behöver för sitt syfte när de faktiskt behöver dessa uppgifter. Intygen innehåller av den anledningen endast den uppgift, i form av person-id, som behövs för att mottagaren skall kunna göra en mottagningskontroll samt för att senare kunna hämta de personuppgifter som behövs (när de behövs).

Att bygga in dataskydd redan i designen av en lösning är något som givetvis alltid har varit en god idé ur ett datasäkerhetsperspektiv. Bland annat för att minimera skadan vid eventuellt systemintrång och/eller dataläckage. I och med att den nya dataskyddsförordningen (GDPR – General Data Protection Regulation) trätt i kraft krävs detta även av lagstiftningen.

Förordningen säger även att man skall utveckla system med dataskydd som standard, vilket innebär att man inte får lov att lagra mer uppgifter än som krävs för att uppfylla syftet med databehandlingen.

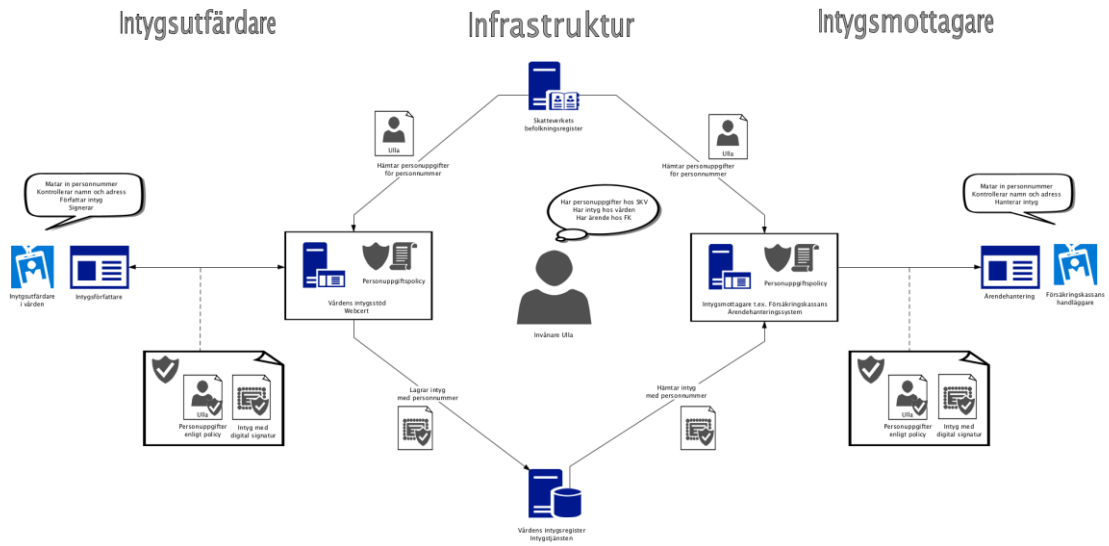
De juridiska aspekterna om inbyggt dataskydd och dataskydd som standard finns att läsa om i artikel 25 av dataskyddsförordningen (GDPR) samt på Datainspektionens webbplats.

### 4.2.3 Force majeure

Då systemet bygger på ständig kontakt med personuppgiftstjänst ställs höga krav på tillgängligheten för denna. I normalfallet är detta inte ett problem då de personuppgiftstjänster som används är centrala komponenter med högt ställda krav på tillgänglighet.

I ett extraordinärt läge av force majeure-karaktär då man inte kan få kontakt med en personuppgiftstjänst för att inhämta personuppgifter finns fortfarande teknisk möjlighet att lösa en del uppgifter med endast personnummer som identifierare. Dock med lägre tillförlitlighet i den mänskliga interaktionen med intyg.

## 4.3 Nuvarande lösning - översikt




Bilden beskriver den lösning som är implementerad och som möjliggör att respektive part kan hantera personuppgifter (och sekretessmarkeringar) i linje med sin lokala personuppgiftspolicy.

Aktuella personuppgifter så som aktuellt namn, adress och sekretessmarkering hämtas vid behov från personuppgiftstjänster som föds av data från Skatteverkets befolkningsregister.

Eftersom intygen inte innehåller namn och adress kan respektive part implementera sin lokala policy för hantering av personuppgifter utan påverkan på övriga parter.

Effekten blir att man alltid har uppdaterade personuppgifter samt att inga personuppgifter exponeras då de inte behövs.

Till vänster i bilden har vi en intygsutfärdare som matar in ett personnummer och med hjälp av personuppgiftstjänsten får namn och adress och därigenom kan verifiera identiteten på intygspersonen. Detta personnummer (person-id) knyts hårt till intyget då intyget signeras. Efter

att intyget signerats är det på grund av den digitala signaturen inte längre möjligt att förändra informationen i intyget inklusive personnummer.

Intygstjänsten lagrar de signerade intygen bundna till en specifik person med hjälp av person-id som kan användas för att identifiera personen och inhämta personuppgifter då de behövs från t.ex. Skatteverket (så som personnummer).

Till höger i bild har vi intygsmottagare som tar emot intygsdata bundna till ett person-id och själva implementerar sin egen policy för hur man hanterar personuppgifter. Då det finns behov av att visa upp personuppgifter, så som namn och adress för intygspersonen, inhämtas dessa vid tillfället från en personuppgiftstjänst och visas för handläggaren som kan verifiera att identiteten stämmer.