Vägledning

Pseudonymisering av personuppgifter

ES2022-01

Juni 2022

Innehåll

1. Inledning

1.1 Syfte med vägledningen

Det finns många frågeställningar runt anonymisering och pseudonymisering. Vad innebär det att anonymisera eller att pseudonymisera och när kan sådan åtgärd öka säkerheten vid en behandling eller öka möjligheterna att behandla information?

Utveckling av nya tjänster och IT-stöd förutsätter behandling av data i någon form. I vissa fall kan behovet av data tillgodoses med ett material som inte innehåller personuppgifter över huvud taget, vilket bör vara en utgångspunkt, men detta är inte alltid möjligt att uppnå. Pseudonymisering av personuppgifter kan minska risken för registrerade och bör användas när så är lämpligt.[1]

Syftet med denna vägledning är att lyfta fram olika scenarier (se avsnitt 5) där pseudonymisering är lämpligt att använda, generellt beskriva de rättsliga förutsättningarna samt ge exempel hur olika organisationer har etablerat lösningar för de olika scenarierna.

Vägledningen utgår från följande användningsområden:

- Ökad säkerhet för personuppgiftsbehandlingen internt inom en offentlig organisation
- Ökad säkerhet för personuppgiftsbehandlingen i relationen med aktörer utanför den egna organisationen, t.ex. leverantörer
- Utökade möjligheter att utbyta information mellan aktörer

1.2 Målgrupp

Vägledningen riktar sig till personer som arbetar med informationshantering, exempelvis verksamhetsutvecklare, verksamhetsarkitekter, specialister inom informationssäkerhet och jurister som arbetar med digitalisering.

1.3 Avgränsningar

Vägledningen är avgränsad till scenarier och rekommendationer för pseudoymisering. Förutsättningar för anonymisering och metoder för detta beskrivs enbart i korthet för att

[1] Se skäl 28, artikel 25 och artikel 32.1a i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (GDPR).

åskådliggöra skillnaden mellan anonymisering och pseudoymisering och någon närmare redogörelse för hur en anonymisering uppnås ingår inte i denna vägledning.

Vägledningen avser pseudonymisering relaterat till personuppgifter. Ibland talas om pseudonymisering av organisationer, detta tas inte upp i denna vägledning.

1.4 Medverkande

Arbetet med att ta fram vägledningen har genomförts av en särskild arbetsgrupp bestående av Christopher-Robin Öunpuu, Désiréé Verschetti, Emil Öhlen, Harriet Schaffer Ullman, Jaan Entson, Jörgen Sannagård, Katarina Lind, Liisa Laukkanen, Linda Lindström, Mikael Österlund, Peter Hammar, Ulf Palmgren och Åsa Kristenssen. Kvalitetssäkring har skett i eSams rättsliga expertgrupp, expertgruppen i säkerhet samt koordineringsgruppen för arkitektur. Beredning har skett via eSams samordningsgrupp.

2. Begrepp och syfte med pseudonymisering

2.1 Begreppen

I denna vägledning har dataskyddsrättsliga begrepp samma betydelse som i dataskyddsförordningen. Notera att i 2 kap. 7 § tryckfrihetsförordningen finns en egen definition av personuppgift.[2]

2.1.1 Personuppgift

Enligt artikel 4 p. 1 dataskyddsförordningen är personuppgifter:

"varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet".

Personuppgifter är således upplysningar som avser en identifierad eller identifierbar fysisk person som är bestämbar och dessa uppgifter omfattas i sin helhet av kraven i dataskyddsförordningen.

Det kan vara fråga om direkta eller indirekta personuppgifter[3] eller en kombination av de två. I många fall är det inte något problem att avgöra vad som är en personuppgift, men det finns fall när det är mer komplicerat (se avsnitt 3.1.2).

2.1.2 Anonymisering

Enligt skäl 26 i dataskyddsförordningen bör principerna för dataskyddet inte gälla anonym information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar.

[2] "Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person."
[3] Namn och personnummer är exempel på direkta personuppgifter. Telefonnummer, registreringsnummer på fordon, diarienummer och IP-adress är exempel på så kallade indirekta personuppgifter. För att veta vilken person som en indirekt personuppgift avser behöver man ytterligare information såsom t.ex. uppgift om vem som är ägare till ett fordon med ett visst registreringsnummer.

Med anonymisering avses att uppgifter om en person behandlas på så sätt att personen inte längre kan identifieras utifrån dessa.

För anonymisering krävs att två förutsättningar är uppfyllda:

- Anonymiseringen är oåterkallelig
- Anonymiseringen har gjorts på ett sådant sätt att det inte går att identifiera den fysiska personen ifråga.

Anonymiserade uppgifter omfattas inte av dataskyddsförordningens bestämmelser. Däremot måste det finnas en rättslig grund för att personuppgifter får anonymiseras. Därtill kan frågor om t.ex. sekretess, upphovsrätt eller säkerhetsskydd aktualiseras.

Anonymiserade uppgifter kan sparas exempelvis av forskningsskäl eller i syfte att föra statistik. Uppgifterna kan t.ex. aggregeras eller ändras till statistisk form på så sätt att uppgifter om en enskild person inte längre är i identifierbar form.

Det finns vissa metoder som relaterar till anonymisering såsom randomisering, generalisering och maskning.[4] Det bör noteras att metoderna har sina begränsningar vad gäller att uppnå anonymisering i dataskyddsförordningens mening.

Randomisering bygger på förändring av uppgifter. Syftet är att avlägsna kopplingen mellan individen och uppgifterna utan att värdet av uppgifterna går förlorat.

Generalisering bygger på att minska uppgifternas detaljnivå. Denna metod kommer bara fungera om flera individers uppgifter lagras tillsammans.

Maskning bygger på att ta bort alla uppenbart personliga identifierare från uppgifterna. Denna metod behöver ofta användas tillsammans med någon av de andra metoderna.

2.1.3 Pseudonymisering

Enligt artikel 4 p. 5 dataskyddsförordningen är pseudonymisering:

"behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person".

[4] Enisas guideline, Data Protection Engineering From Theory to Practice, Januari 2022 samt artikel 29-gruppens Yttrande 05/2014 om avidentifieringsmetoder, WP216 (ej ratificerat av Europeiska dataskyddsstyrelsen (EDPB)).

Det följer av definitionen i artikel 4 samt skäl 26 dataskyddsförordningen att pseudonymiserade personuppgifter fortfarande ska ses som personuppgifter, eftersom personer genom dem är identifierbara.

Rättsliga förutsättningar för pseudonymisering beskrivs i avsnitt 3.2.

2.1.4 Avidentifiering

Ett vanligt förekommande begrepp i de sammanhang som tas upp i denna vägledning är *avidentifiering*. Detta begrepp används dels som ett samlingsnamn för både anonymisering och pseudonymisering, dels enbart för anonymisering, vilket kan leda till missförstånd om vad som avses. Därmed används inte detta begrepp i denna vägledning.

2.1.5 Kompletterande uppgifter

Beståndsdelarna i en pseudonymisering, dvs. de kompletterande uppgifterna enligt artikel 4 p. 5 dataskkyddsförordningen, kan benämnas på olika sätt.

När det är fråga om en pseudonymiseringsmetod med utformning Olle = 1, se avsnitt 4.3.1.1, kallas de kompletterande uppgifterna ofta översättningstabell, kopplingsregister, kopplingstabell eller täcknamn. Inom forskningsområdet benämns dock den kompletterande uppgiften vanligen som kodnyckel.

I en pseudonymiseringsmetod där krypteringsalgoritm används benämns vanligen de kompletterande uppgifterna som kodnyckel, krypteringsnyckel, behörighetsnyckel, etc., se avsnitt 4.3.1.2.

Således förekommer begreppet kodnyckel eller nyckel för den kompletterande uppgiften i båda metoderna. Det är inte heller ovanligt att metoderna kombineras och då används ibland begreppet kodnyckel för den kombinerade metoden.

I denna vägledning används genomgående begreppen kompletterande uppgifter och nyckel och avser då kompletterande uppgifter oavsett pseudonymiseringsmetod.

2.2 Syftet med pseudonymisering

Grundsyftet med pseudonymisering är att minska möjligheten att koppla olika uppgifter eller uppgiftssamlingar till en levande fysisk person och skydda den enskildes integritet. Genom pseudonymisering delas data om personen upp i åtskilda delar.

Pseudonymisering kan utgöra ett användbart verktyg för att säkerställa förenlighet med dataskyddsförordningen och möjliggöra behandling av personuppgifter som annars inte

hade varit tillåten, t.ex. i vissa fall vid tredjelandsöverföring. Pseudonymisering kan också användas som säkerhetsåtgärd vid behandling av personuppgifter. Pseudonymisering kan t.ex. öka säkerheten för personuppgiftsbehandlingen inom en organisation i relation till aktörer utanför den egna organisationen.

Pseudonymisering ger möjlighet att behålla kopplingen mellan pseudonym och data som innehåller grundidentiteter vilket betyder att det går att koppla historisk och framtida information samt skapa serier över tid.

3. Rättsliga förutsättningar

3.1 Skillnaden mellan pseudonymisering och anonymisering

Skillnaden mellan pseudonymisering och anonymisering avgörs utifrån om det är möjligt att identifiera den fysiska personen eller inte. Pseudonymiserade personuppgifter omfattas fortfarande av dataskyddsregelverket till skillnad från anonymiserade uppgifter. Pseudonymisering är således inte en metod för anonymisering.

3.1.1 Identifierbar fysisk person

För att det ska föreligga en anonymisering ska det inte gå att identifiera den fysiska personen ifråga. Identifiering av personen måste förhindras på ett oåterkalleligt sätt och på ett sådant vis att den som hanterar uppgifterna eller någon utomstående aktör inte längre kan ändra tillbaka uppgifter som den innehar till identifierbar form. Att bara ta bort uppgift om namn och andra specifika uppgifter om en person innebär inte alltid att alla uppgifter om personen blir anonyma. Ett material kan innehålla mer specifika detaljer, t.ex. uppgift om en ovanlig diagnos, vilken gör att personen indirekt kan identifieras. Även en annan aktör skulle kunna utläsa vem personen är med hjälp av egna uppgiftssamlingar.

Förutsättningarna för när en person är identifierbar anges i skäl 26 i dataskyddsförordningen. För att bedöma om en person är identifierbar ska alla tillgängliga ”hjälpmedel”[5] beaktas och det ska också bedömas om dessa med ”rimlig sannolikhet” kan komma att användas för att identifiera personen. Samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, liksom såväl tillgänglig teknik som den tekniska utvecklingen ska beaktas, vilket innebär en utmaning i bedömningen. Förändrad teknik skulle kunna innebära att enskilda kan bli identifierbara utifrån uppgifter som bedömts vara anonyma. Det är svårt att säga var gränsen går för när en uppgift ska anses vara anonymiserad. Det får avgöras utifrån förutsättningarna i varje enskilt fall. Med dagens teknik är det ofta möjligt att återskapa kopplingen så länge datat som innehåller grundidentiteter finns kvar. Förutsättningarna är att uppnå anonymisering är därmed små.

Kan en fysisk person identifieras är det fråga om personuppgifter.

[5] Hjälpmedel kan exempelvis vara lagstiftning som möjliggör tillgång till information, tekniska metoder, etc.

3.1.2 En och samma personuppgift i förhållande till olika aktörer

En intressant fråga är om bedömningen av om en person är identifierbar (och det därmed är fråga om en personuppgift) kan skilja sig åt för olika aktörer. EU-domstolens har i Breyer-målet[6] prövat frågan om uppgifter kan anses vara personuppgifter hos en aktör A men inte i förhållande till en annan aktör B. Målet avsåg dynamiska IP-adresser som inte gjorde det möjligt att skapa en koppling mellan en viss dator och den fysiska anslutningen till nätverket som den aktuella internetleverantören använde genom handlingar tillgängliga för allmänheten. I målet argumenterades[7] för att de dynamiska IP-adresserna utgjorde personuppgifter för internetleverantören eftersom adresserna gjorde det möjligt för denne att identifiera användaren. Däremot argumenterades det att IP-adresserna inte skulle utgöra personuppgifter i förhållande till den som driver de webbplatser som personen besökt. Som grund för argumentation framfördes att de som driver webbplatserna, i det fall personen inte uppgett sin identitet under besöken på webbplatserna, inte förfogade över de upplysningar som var nödvändiga för att identifiera personen i fråga utan överdriven ansträngning. EU-domstolen tog ställning till om möjligheten att kombinera en dynamisk IP-adress med ytterligare information som internetleverantören innehade utgjorde ett hjälpmedel som rimligen kunde komma att användas av webbsideinnehavaren för att identifiera den aktuella personen. Domstolen uttalade att så inte skulle vara fallet om identifiering av den aktuella personen skulle vara förbjuden i lag eller omöjlig att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft, med den följden att risken för identifiering i praktiken var försumbar. Enligt domstolen föreföll det i tysk rätt finnas lagliga medel som gjorde det möjligt för webbsideinnehavare att kunna få upplysningar från internetleverantörer. EU-domstolen bedömde mot den bakgrunden att en dynamisk IP-adress som en webbsideinnehavare registrerar i samband med besök på webbplatsen utgör en personuppgift i förhållande till webbsideinnehavaren, när det finns lagliga medel som gör det möjligt för denne att identifiera den registrerade med hjälp av ytterligare upplysningar som den registrerades internetleverantör förfogar över.

I domen tas utgångpunkt i vad som är möjligt att på laglig väg ta del av i form av ytterligare upplysningar som kan möjliggöra en identifiering.[8] Motsatsvis bör då uppgifterna inte anses vara personuppgifter för de som inte utifrån tillgängliga hjälpmedel och en rimlig arbetsinsats har möjlighet att genomföra en identifiering av fysiska personer.

[6] EU-domstolens dom (andra avdelningen) av den 19 oktober 2016, Patrick Breyer mot Bundesrepublik Deutschland, C-582/14.
[7] Dvs argumentation som framförts i målet i den nationella domstolen.
[8] Jfr även Generaladvokatens förslag p 70-73.

Således kan personuppgifter utgöra personuppgifter i förhållande till aktör A medan de inte anses utgöra personuppgifter i förhållande till aktör B om det föreligger ett förbud för aktör B att ta del av ytterligare uppgifter som möjliggör en identifiering. Detsamma gäller om en identifiering är omöjligt att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft. Detta rekvisit är mer svårbedömt och vad som är en orimlig resurs bör bli beroende på aktörens förmåga.

3.2 Förutsättningar för pseudonymisering

3.2.1 Separat förvaring samt tekniska och organisatoriska åtgärder

Som tidigare framhållits utgör pseudonymiserade personuppgifter fortfarande personuppgifter i den mening som avses i dataskyddsförordningen. En personuppgiftsansvarig måste alltså även efter det att personuppgifter pseudonymiserats iaktta de grundläggande principerna som följer av förordningens artikel 5, såsom principerna om uppgifts- och lagringsminimering, samt tillse att behandlingen alltjämt uppfyller kraven på rättslig grund i artikel 6. En pseudonymisering utesluter inte heller att andra tekniska och organisatoriska åtgärder enligt artikel 32 kan behövas, exempelvis i form av behörighetsstyrning och loggning av åtkomst till de pseudonymiserade personuppgifterna. Även övriga krav i dataskyddsförordningen måste vara uppfyllda.

Förutsättningarna för att personuppgifter ska anses vara pseudonymiserade framgår av artikel 4 p. 5 i dataskyddsförordningen. Personuppgifterna ska enligt artikeln inte längre kunna tillskrivas en specifik registrerad utan att kompletterande uppgifter används. Detta gäller endast under förutsättning att de kompletterande uppgifterna som kan identifiera fysiska personer förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att identifiering inte sker. Genom att på detta sätt förhindra att vissa data kopplas till en viss specifik registrerad person kan riskerna för de registrerade minskas.

I avsnitt 4 beskrivs olika metoder för pseudonymisering.

3.2.2 Pseudonymisering i förhållande till offentlighetsprincipen

För en svensk myndighet som överväger att pseudonymisera uppgifter uppstår den principiellt intressanta frågan om det skydd som åtgärden förutsätts medföra i praktiken inskränks genom regelverket om handlingsoffentlighet. En förutsättning för pseudonymisering är att de kompletterande uppgifterna förvaras separat på ett sådant sätt att en fysisk person inte kan identifieras. Kan det föreligga en risk för att det anses

att sådan separat förvaring inte föreligger om de kompletterande uppgifterna skulle behöva lämnas ut vid en begäran om utlämnande av allmän handling? För att kunna avgöra i vilka situationer det finns förutsättningar att använda pseudonymisering som en effektiv dataskyddsåtgärd hos en myndighet, behöver närmare utredas hur åtgärden förhåller sig till offentlighetsprincipen och sekretesslagstiftningen.

Offentlighetsprincipen är central i den svenska rättsordningen och uttrycks bl.a. i tryckfrihetsförordningen (1949:105) (TF) där rätten att ta del av allmänna handlingar regleras (2 kap). Denna rätt kan begränsas genom sekretess. Regeringen har utifrån artikel 86[9] samt skäl 154[10] i dataskyddsförordningen funnit[11] att den EU-rättsliga dataskyddsregleringen inte inkräktar på den grundlagsreglerade offentlighetsprincipen. Den sammanjämkning som nämns i dataskyddsförordningen kommer till uttryck i svensk rätt bl.a. genom bestämmelserna i offentlighets- och sekretesslagen (2009:400) (OSL) som är resultatet av noggranna avvägningar mellan allmänhetens intresse av insyn i det allmännas verksamhet och den enskildes behov av skydd för sin personliga integritet. I 1 kap. 7 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning anges att varken dataskyddsförordningen eller kompletterande bestämmelser ska tillämpas i den utsträckning det skulle strida mot TF eller yttrandefrihetsgrundlagen (1991:1469) (YGL).

3.2.2.1 De kompletterande uppgifterna kan vara en allmän handling

En fråga som uppkommer är om de kompletterande uppgifterna (se avsnitt 2.1.5 om att vanliga benämningar på de kompletterande uppgifterna är kodnyckel, översättningstabell, täcknamn m.m.) är en handling och om det i så fall är fråga om en allmän handling.

Med handling förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med ett tekniskt hjälpmedel. En handling är allmän, om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos en myndighet (2 kap. 9 – 10 §§ TF). Det finns även särskilda regler för överlämnande av handling inom samma myndighet (2 kap. 11 § TF) samt om minnesanteckningar (2 kap. 12 § TF). En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses enligt 2 kap. 13 § inte som allmän handling hos den myndigheten. Vidare anses

[9] Av artikel 86 i dataskyddsförordningen framgår att personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.
[10] I skäl 154 anges bland annat att dataskyddsförordningen gör det möjligt att vid tillämpningen av den samme ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Det anges vidare att den nationella rätten bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd för personuppgifter.
[11] Prop. 2017/18:105.

enligt 2 kap. 14 § bl.a. inte en upptagning som allmän handling, om upptagningen förvaras hos en myndighet där den ursprungliga handlingen inte skulle vara att anse som allmän.

Som beskrivits i avsnitt 4 kan pseudonymisering, beroende på vilken metod som används, bestå av olika beståndsdelar. Det behöver därför analyseras vad det är för information som kommer att skapas, om det skapas handlingar i processen och om de är allmänna. Man behöver t.ex. bedöma om de kompletterande uppgifterna förvaras hos myndigheten. I många fall bör så vara fallet. Det kan konstateras att lagstiftaren tagit höjd för att kodnycklar kan komma att bedömas som allmänna handlingar, jfr 18 kap. 9 § OSL (se avsnitt 3.2.2.3 nedan). I fall där pseudonymiseringen utförs av en extern aktör kan det finnas anledning att fundera kring undantaget om teknisk bearbetning och lagring utifrån handlingens läsbarhet. Det vill säga om det är möjligt att utföra pseudonymiseringen i ett system där inte handlingarna finns i läsbart skick för mer än systemadministratören och för viss support så att hanteringen kan anses omfattas av undantaget i 2 kap. 13 § TF. I denna vägledning har inte närmare analyserats i vilken omfattning undantaget skulle kunna vara tillämpligt.

Frågan om de kompletterande uppgifterna är att anse som allmän handling behöver bedömas i varje enskilt fall. Det framstår dock som sannolikt att de kompletterande uppgifterna kommer att utgöra en allmän handling eller uppgifter i sådan. En myndighet bör därmed som utgångspunkt utgå från detta när den avser att tillämpa pseudonymisering.

3.2.2.2 Allmänt om sekretess

Rätten att ta del av allmänna handlingar får endast begränsas om det är påkallat med hänsyn till vissa angivna intressen. Sekretess gäller både i förhållande till enskilda och mellan myndigheter, men också inom en myndighet, om det där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1-2 §§ OSL). Sekretess gäller även mot utländska myndigheter och mellanfolkliga organisationer (8 kap. 3 § OSL). En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, dvs. förutsättningar för bestämmelsens tillämplighet. Dessa tre rekvisit anger sekretessens föremål, sekretessens räckvidd och sekretessens styrka.

Sekretessens föremål är den information som kan hemlighållas, en sekretessbestämmelses räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet och sekretessens styrka bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit.

Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att utlämnandet av uppgiften kommer att leda till någon form av skada eller men för den uppgiften berör. Vid ett omvänt skaderekvisit gäller sekretess om det inte står klart att uppgiften kan röjas utan att viss skada uppkommer. En del bestämmelser innehåller ett kvalificerat rakt skaderekvisit. Det innebär att det krävs särskilt mycket för att sekretessen ska gälla. Sekretessen enligt en bestämmelse kan även vara absolut. I ett sådant fall ska de uppgifter som omfattas av bestämmelsen hemlighållas utan någon skadeprövning om uppgifterna begärs utlämnade. Sekretessmarkering innebär inte att handlingen per automatik är ”hemligstämplad”. Det är enbart en indikation på att den som har handlingen i sin vård behöver göra en sekretessbedömning.

3.2.2.3 Sekretessbestämmelser som kan aktualiseras

Beroende av vad det är som begärs ut kan olika sekretessbestämmelser bli aktuella att tillämpa. I det följande behandlas ett antal olika sekretessbestämmelser för att undersöka dess tillämplighet vid en sådan begäran om utlämnande. I vissa fall kan flera sekretessbestämmelser aktualiseras samtidigt. Observera att en prövning alltid måste göras i varje enskilt fall som uppgifter begärs utlämnade.

Verksamhets- och ärendespecifika sekretessregler
I offentlighets- och sekretesslagen finns sekretessregler som gäller för en viss verksamhet eller viss ärendehandläggning hos en myndighet. Enligt eSams uppfattning bör de kompletterande uppgifterna anses kunna ha sådan nära koppling till de pseudonymiserade uppgifterna att sådana regler i pseudonymiseringsfallen även bör kunna omfatta de kompletterande uppgifterna. Exempelvis bör sekretess enligt 28 kap. 1 § OSL för uppgifter om hälsotillstånd och andra personliga förhållanden i verksamhet hos Försäkringskassan och Pensionsmyndigheten kunna gälla de kompletterande uppgifterna vid en pseudonymisering. Likaså får kompletterande uppgifter som har koppling till uppgifter som omfattas av statistiksekretess enligt 24 kap. 8 § OSL också anses omfattas av den bestämmelsen.[12]

18 kap. 9 § OSL
Bestämmelsen i 18 kap. 9 § 1 OSL som avser uppgift om chiffer, kod eller liknande metod, kan vara aktuell att tillämpa vid pseudonymisering av personuppgifter. Som framgår av bestämmelsen krävs, för att en uppgift om viss metod ska vara skyddad av sekretess, att metoden har till syfte att underlätta befordran eller användning i allmän verksamhet av i och för sig sekretessbelagda uppgifter. I lagförarbetena framhålls kryptering som ett exempel på en metod som används för detta syfte.

[12] Prop. 1979/80:2 Del A s. 263 och prop. 2020/21:124 s. 59 f.

Krypteringsnyckeln eller koden är vid sådan användning skyddat av sekretess enligt bestämmelsen.[13] Även pseudonymisering utgör en metod som kan ha detta syfte och därmed omfattas av bestämmelsen. Om sekretess gäller för uppgifter om enskilda där pseudonymisering använts, kommer de kompletterande uppgifterna att skyddas av sekretess enligt nu aktuell bestämmelse. Motsatsvis gäller att i de fall personuppgifterna i sig inte omfattas av sekretess, omfattas inte heller de kompletterande uppgifterna av sekretess.[14] Förutom de kompletterande uppgifterna i sig kan sekretessen enligt lagstiftaren också avse andra uppgifter om metoderna, t.ex. dokumentation om vilka metoder för kryptering som används.[15] Detsamma bör enligt eSams uppfattning gälla för pseudonymiseringsmetoder.

Sekretessen enligt 18 kap. 9 § OSL är begränsad med ett rakt skaderekvisit. Det föreligger således en presumtion för offentlighet. Det framstår dock som uppenbart att syftet med pseudonymisering motverkas om kodnyckeln röjs och enligt eSams uppfattning bör därför bestämmelsen vanligen kunna bli tillämplig. För att pseudonymiseringen ska ha avsedd effekt måste dessa uppgifter kunna hemlighållas.

18 kap. 8 § 3 OSL

Enligt 18 kap. 8 § 3 OSL gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information. Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas.[16] Sekretessen gäller i första hand uppgifter om behörighetskoder och behörighetsnycklar för tillgång till uppgifter som upptagits genom automatiserad behandling samt arrangemang och fördelning av dessa. Behörigheten kan avse tillgång till upptagningar som är offentliga. Sekretessen kan skydda dessa upptagningar mot manipulationer i form av obehöriga tillägg, raderingar eller förvanskningar. Sekretesskyddet gäller behörigheten att få tillgång till andra handlingar och kan gälla exempelvis för en låskod till ett förvaringsrum för hemliga handlingar. Med ett rakt skaderekvisit följer som huvudregel en presumtion för offentlighet. Bestämmelsen bör enligt eSams uppfattning ändå kunna aktualiseras vid begäran om utlämnande av kompletterande uppgifter. Kammarrätten i Stockholm har i ett mål som rörde uppgift om källkod funnit att uppgifterna omfattades av sekretess enligt bestämmelsen.[17]

[13] Prop. 1979/80:2 Del A s. 143.
[14] Prop. 2017/18:298 s. 73.
[15] Prop. 2012/13:128 s. 56.
[16] Prop. 2003/04:93, 2003/04:KU17.
[17] Kammarrättens i Stockholm dom i målnr 3692-19.

21 kap. 7 § OSL

Enligt 21 kap. 7 § OSL gäller sekretess för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning eller 6 § lagen (2003:460) om etikprövning av forskning som avser människor. Av ett kammarrättsavgörande angående utlämnande av allmän handling framgår att domstolen anser att bestämmelsen, i enlighet med vad som anges i förarbetena, ska tolkas på så sätt att sekretess gäller om myndighetens utlämnande av uppgiften står i strid med bestämmelserna om överföring till tredje land. Även sökandens efterföljande behandling av uppgifterna ska anses omfattas av bestämmelsen.[18] Av praxis följer att bestämmelsen enbart tar sikte på mottagarens behandling av personuppgifterna.[19] Det som ska bedömas enligt bestämmelsen är alltså endast om mottagarens avsedda behandling av de personuppgifter som begärs ut uppfyller kraven enligt dataskyddsförordningen. Enligt JO:s uttalande (dnr 1102–2004) får vidare undersökningar om mottagarens behandling vidtas endast om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, t.ex. massuttag eller selekterade uttag. Finns det inga sådana indikationer behöver inte någon bedömning enligt dataskyddsregleringen göras. eSams bedömning är att bestämmelsen har en mer begränsad tillämpning vid begäran om utlämnande av de kompletterande uppgifterna.

3.2.2.4 Föreligger förutsättningar för pseudonymisering utifrån offentlighetsprincipen och gällande sekretessregler?

Som framgår av redogörelsen av sekretessbestämmelser ovan finns det ett antal bestämmelser som kan aktualiseras vid en begäran om utlämnande av de kompletterande uppgifterna (se avsnitt 2.1.5 om att vanliga benämningar på de kompletterande uppgifterna är kodnyckel, översättningstabell, täcknamn m.m.). I de fall det är fråga om absolut sekretess finns ett förbud för ett utlämnande. När det gäller omvänt skaderekvisit och rakt skaderekvisit tillkommer en skadeprövning som innebär att en myndighet måste pröva förutsättningarna för ett utlämnande. Ytterst kan alltid ett myndighetsbeslut om att inte lämna ut en allmän handling överprövas av domstol och utgången kan bli en annan, varför det kan sägas föreligga en risk för att uppgifterna inte förvaras separat på ett sådant sätt att en fysisk person inte kan identifieras. Ett sådant resonemang skulle dock få konsekvensen att pseudonymisering aldrig skulle kunna användas som ett lämpligt verktyg om de kompletterande uppgifterna anses vara en offentlig allmän handling. Istället bör man kunna argumentera för att sekretesslagstiftningen till sin utformning är avsedd att ge ett tillräckligt skydd oavsett grad av sekretess (absolut,

[18] Kammarrättens i Stockholm dom i målnr 7299-10.
[19] HFD 2014 ref. 66.

omvänd och rak). eSams bedömning är offentlighetsprincipen inte begränsar möjligheterna att göra en pseudonymisering.

3.2.3 Hantering av kompletterande uppgifter

Som konstaterats i 3.2.2.1 behöver det bedömas i varje enskilt fall om de kompletterande uppgifterna anses vara en allmän handling, men att det framstår som sannolikt att de kompletterande uppgifterna kommer att bedömas som en allmän handling eller uppgifter i sådan. En myndighet bör därmed som utgångspunkt utgå från detta när den avser att tillämpa pseudonymisering. Vid pseudonymisering kommer det därmed finnas flera beståndsdelar som var och en utgör en handling, såsom datat som innehåller grundidentiteter, det pseudonymiserade datat och de kompletterande uppgifterna (nyckeln).

Det ankommer på en myndighet att besluta om det är allmänna handlingar som ska registreras eller förvaras i särskild ordning, 5 kap. 1 § OSL. Myndigheten behöver också säkerställa förutsättningarna för arkivering och gallring.

3.2.3.1 Dataskyddsförordningen och arkiv

Artikel 5 i dataskyddsförordningen innehåller grundläggande principer för behandling av personuppgifter. Av principerna framgå bl.a. att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. I denna bestämmelse anges vidare att personuppgifter får lagras under längre tid i den mån som personuppgifterna behandlas för t.ex. arkivändamål av allmänt intresse.

All behandling av personuppgifter måste vila på en rättslig grund. Av artikel 6 p. 3 dataskyddsförordningen framgår att vad som är arkivändamål av allmänt intresse ska fastställas i nationell rätt eller i unionsrätten. Sverige har för myndigheter fastställt vad som utgör arkivändamål av allmänt intresse i arkivlagen (1990:782). Av 1 kap. 6 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, framgår att bestämmelser i en annan lag ska tillämpas om de avviker från denna lag. Därmed ska arkivlagens bestämmelser tillämpas före lagen om kompletterande bestämmelser.

3.2.3.2 Förutsättningar för gallring

Allmänna handlingar hos myndigheter och offentliga organisationer ska arkiveras och bevaras. Bestämmelser om detta finns i arkivlagen. Myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser följande ändamål; (1) rätten att ta del av allmänna handlingar, (2) behovet av information för rättskipningen och förvaltningen,

och (3) forskningens behov. Allmänna handlingar får gallras, under förutsättning att det arkivmaterial som återstår efter gallring ska kunna tillgodose ändamålen (10 § arkivlagen).

Riksarkivet får meddela föreskrifter om gallring och om föreskrifter saknas får Riksarkivet meddela särskilda beslut om gallring (12 § arkivförordningen [1991:446}). Statliga myndigheter får gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet om inte särskilda gallringsföreskrifter finns i lag eller förordning (14 §).

Gallringsbestämmelser finns i flera myndigheters registerförfattningar. Ett exempel på sådan reglering är lagen (2001:99) och förordningen (2001:100) om den officiella statistiken. I 19 § i lagen finns en generell gallringsbestämmelse. Enligt bestämmelsen kan regeringen bemyndiga en myndighet att till för forskningens behov föreskriva om undantag från denna gallringsföreskrift. Riksarkivet har fått sådant bemyndigande och beslutat flera förskrifter om undantag från gallring hos SCB i RA-MS-serien (myndighetsspecifika föreskrifter om gallring).

Bevarande eller gallring av kompletterande uppgifter måste hanteras på samma sätt som gallring av uppgifter ur arkiven generellt. Myndigheten behöver utreda och ta ställning till om de kompletterande uppgifterna kan behövas i framtiden för att förstå andra uppgifter i arkivet, dvs. om de behövs för rättsskipningen eller förvaltningen eller om det finns det ett värde för framtida forskning. Utgångspunkten för utredningen är 3 § arkivlagen.

Gallring av kompletterande uppgifter täcks inte av Riksarkivets generella föreskrifter (RA-FS) vilket innebär att en myndighet som vill kunna gallra en sådan uppgift behöver göra en framställan om gallring till Riksarkivet. Efter Riksarkivets prövning kan myndigheten få en myndighetsspecifik föreskrift om gallring (RA-MS).

Det bör vara möjligt att fastställa att de uppgifter som använts vid en utredning eller forskningsarbete varit relevanta och korrekta på annat sätt än att det måste finnas möjlighet att ta del av den kompletterande uppgiften. Det bör därför många gånger kunna bedömas att uppgiften inte behöver bevaras. Det kan finnas tillfällen där behov av längre bevarande finns, t.ex. vid återkommande forskningsstudier som görs med långa intervall, såsom att följa en population över tid.

3.2.4 Pseudonymisering vid överföring av personuppgifter till ett tredje land

Som angetts i inledningen till denna vägledning kan pseudonymisering ha användningsområden när det kommer till tredjelandsöverföringar. Frågor om sådan tillämpning har särskilt aktualiserat efter den s.k. Schrems II-domen.[20]

Enligt dataskyddsförordningen ligger ett stort ansvar på en personuppgiftsansvarig som avser att överföra personuppgifter till mottagare i ett tredje land. En sådan överföring kan exempelvis grundas på s.k. standardavtalsklausuler, men beroende på lagstiftningen i det tredje land dit en överföring ska ske kan klausulerna behöva kompletteras med ytterligare skyddsåtgärder för att uppnå den skyddsnivå som krävs enligt unionsrätten. Europeiska dataskyddsstyrelsen (EDPB) har antagit rekommendationer[21] om sådana ytterligare skyddsåtgärder i syfte att hjälpa den som överför eller överväger att överföra personuppgifter till ett tredje land.

I en bilaga till rekommendationerna ges exempel på skyddsåtgärder i form av tekniska, organisatoriska och avtalsmässiga åtgärder samt användningsfall som beskriver när de kan användas. Skyddsåtgärderna måste vara *effektiva* i den mening som avses i EU-domstolens avgörande i Schrems II. En skyddsåtgärd är enligt rekommendationerna effektiv i denna mening endast om den, ensamt eller tillsammans med andra åtgärder, avhjälper de specifika brister som har identifierats i bedömningen av det tredje landets lagstiftning som påverkar överföringen.[22]

EDPB anger att pseudonymisering utgör en effektiv skyddsåtgärd under vissa förhållanden. För att åtgärden ska vara effektiv krävs enligt EDPB att:

1. uppgiftsutföraren överför personuppgifter som har behandlats på ett sådant sätt att uppgifterna inte längre kan tillskrivas en specifik registrerad person eller användas för att skilja ut den registrerade ur en större grupp utan användning av ytterligare uppgifter,
2. dessa ytterligare uppgifter helt och hållet innehas av uppgiftsutföraren och hålls avskilt i en medlemsstat eller i ett tredjeland, av en aktör som är betrodd av uppgiftsutföraren inom EES eller inom en jurisdiktion som erbjudet ett i väsentliga delar likvärdigt skydd som inom EES,
3. utlämning eller otillåten användning av dessa ytterligare uppgifter förhindras med lämpliga tekniska och organisatoriska skyddsåtgärder som säkerställer att

[20] C-311/18, EU-domstolens dom (stora avdelningen) av den 16 juli 2020. Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems.
[21] Europeiska dataskyddsstyrelsens (EDPB:s) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.
[22] Rekommendationerna punkt 75.

uppgiftsutföraren behåller egen kontroll över algoritmen eller datakatalogen som möjliggör återidentifiering med hjälp av de ytterligare uppgifterna och

4. den personuppgiftsansvarige genom en noggrann analys av de ifrågavarande uppgifterna har fastställt – med hänsyn tagen till all information som de offentliga myndigheterna i mottagarlandet kan förväntas inneha och använda – att de pseudonymiserade personuppgifterna inte kan tillskrivas en identifierad eller identifierbar fysisk person även om korshänvisningar görs till sådana uppgifter.[23]

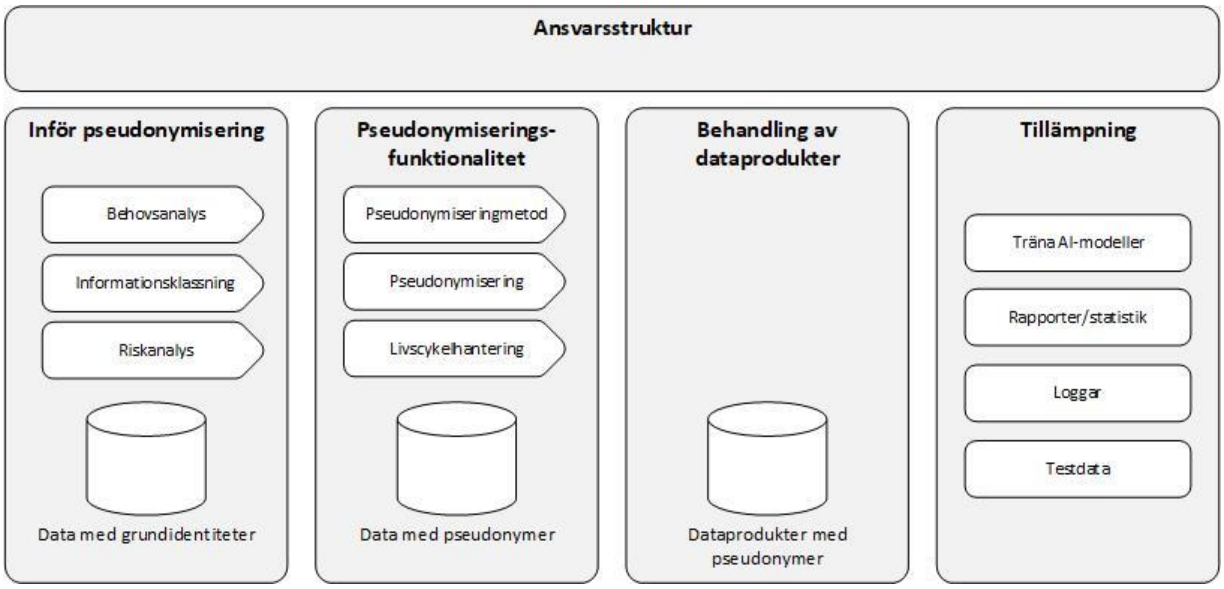
Av rekommendationerna följer att pseudonymisering inte kan utgöra en effektiv skyddsåtgärd i situationer där mottagaren, t.ex. en molntjänstleverantör, måste ha tillgång till personuppgifterna i klartext för att utföra avtalade uppgifter och där mottagarlandets myndigheters rätt till tillgång till uppgifterna går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle. eSam delar denna bedömning.

[23] A.a. p. 85.

4. Pseudonymisering

Användandet av pseudonymisering förutsätter att:

- Ansvarsstrukturen är tydlig
- Åtgärder vidtas inför pseudonymiseringen
- Pseudonymiseringsfunktionalitet etableras och vidmakthålls



Resultatet från pseudonymiseringen bidrar till att skapa och behandla olika dataprodukter där pseudonymer används som ersättning för grundidentiteterna tillsammans med övrig information som behövs för aktuellt användningsområde. Dataprodukterna används i sin tur inom olika tillämpningar, exempelvis för att träna AI-modeller eller i statistikändamål. I de följande avsnitten beskrivs frågor kring ansvarsstruktur, åtgärder att vidta inför pseudonymisering samt pseudonymiseringsfunktionalitet.

4.1 Ansvarsstruktur

Vid en pseudonymisering behöver roller och ansvarsområden för olika parter i ett scenario definieras. För mer detaljerade definitioner se bl.a. guidelines från EDPB[24] och European Union Agency for Cybersecurity (Enisa).[25] Vanligt förekommande roller är:

[24] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR Version 2.0 Antaget den 7 juli 2021
[25] Pseudonymisation techniques and best practices Recommendations on shaping technology according to data protection and privacy provisions November 2019.

Personuppgiftsansvarig: Ansvarig för behandlingen av personuppgifterna och är den som fastställer behandlingsändamålet och behandlingssättet, dvs. varför och hur en behandling ska utföras. Det finns ingen begränsning vad gäller typen av enhet som kan åta sig rollen som personuppgiftsansvarig, men i praktiken är det vanligen själva organisationen och inte en individ inom organisationen.

Personuppgiftsbiträde: En separat enhet i relation till den personuppgiftsansvarige och som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Inom en organisation finns ofta också utpekade roller som ansvarar för olika delar av genomförandet av en pseudonymisering. Det finns ofta en roll som har till uppgift att godkänna tänkta behandlingar så att dessa är förenliga med verksamhetens uppdrag, sker i enlighet med lagstiftningen och att riskerna med bearbetningen kan rättfärdigas. I rollen ligger också vanligen att säkerställa att det genomförs en informationssäkerhetsklassning och riskanalys. Rollen kallas ibland *informationsägare*. Det finns också ofta utpekat vem som genomför pseudonymiseringen (kan även vara en extern aktör). Därtill finns vanligen också en roll för den som innehar och använder pseudonymiserat data, denna roll kallas ibland *databehandlare*.

I de fall de pseudonymiserade uppgifterna överlämnas från en organisation till en annan kan rollerna uppstå både hos den avsändande organisationen och den mottagande.

4.2 Inför pseudonymisering

I vissa fall kan en pseudonymisering innebära att nyttan med behandlingen minskar om pseudonymiseringen innebär en alltför stor påverkan på resultatet. T.ex. kan användandet av en pseudonymiserad uppgiftssamling vid träning av en AI-modell innebära att algoritmen blir sämre vilket medför att AI-modellen bli sämre än om den hade tränats på data som innehåller grundidentiteter.[26] I vilken omfattning pseudonymisering ska ske förutsätter därför en avvägning mellan risk och nytta. En behovsanalys behöver ligga till grund för användandet av pseudonymisering.

Inför en pseudonymisering behöver det alltid göras en bedömning av vilken information som berörs och en myndighet måste genomföra en informationsklassning utifrån gällande lagstiftning och myndighetens egna regler på området. Det finns lite olika metoder för hur en sådan kan ske.[27] Beskrivning av hur en informationsklassning går till omfattas inte av denna vägledning.

[26] Senavirathne Navoda, Towards privacy preserving Micro-data analysis, A machine learning based perspective under prevailing privacy regulations, Skövde Universitet
[27] Se t.ex. MSBs föreskrifter eller exempel från den kommunala sektorn, KLASSA.

Inför en pseudonymisering behöver det också genomföras en riskanalys. Riskanalys ska göras för att säkra att risker och hot kopplat till informationssäkerheten är identifierade inför en förändring av till exempel en systemlösning, ett arbetssätt eller ett informationsflöde, vilket ett införande av pseudonymisering innebär.

Syftet med riskanalysen är att:

- Kartlägga vilka risker som kan finnas vid en viss hantering av information
- Bedöma risker genom att uppskatta sannolikhet och eventuell skada om hot och händelser inträffar
- Ta fram en handlingsplan på åtgärder som kan minimera de kartlagda riskerna.

Riskanalys är en central del vid införandet av pseudonymisering. Metoderna för sådan riskanalys beskrivs inte i detta dokument. I sammanhanget måste man också överväga om en s.k. konsekvensbedömning behöver göras, jfr artikel 35 i dataskyddsförordningen.

För tillämplig lagstiftning som rör informationssäkerhet, se eSams checklista för jurister.[28]

4.3 Pseudonymiseringsfunktionalitet

Följande funktionalitet behöver kunna tillhandahållas för att etablera en pseudonymisering:

- Användande av lämplig pseudonymiseringsmetod
- Pseudonymisering av grundidentiteter
- Livscykelhantering av pseudonymer

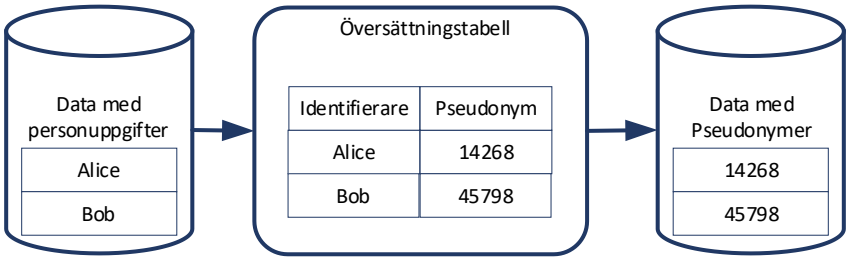
4.3.1 Pseudonymiseringsmetoder

Det finns olika lösningar och tillämpningar för pseudonymiseringsmetoder. I nedan avsnitt beskrivs några av de metoder som är vanligt förekommande. För ytterligare metoder, se Enisas guidelines och rekommendationer.[29] Dessa pseudonymiseringsmetoder kan i vissa fall också kombineras med metoder för anonymisering, se avsnitt 2.1.2 om anonymiseringsmetoder. Användandet av anonymiseringsmetoder är avgränsat från denna vägledning.

[28] Checklista för jurister, Introduktion i rättsliga förutsättningar i utvecklingsinsatser, version 2.0. eSam juni 2019.
[29] Data Pseudonymisation: Advanced Techniques & use cases Technical analysis of cybersecurity measures in data protection and privacy January 2021.
Pseudonymisation techniques and best practices Recommendations on shaping technology according to data protection and privacy provisions November 2019.

4.3.1.1 Översättningstabell

Metoden innebär att att det skapas en pseudonym för en riktig identitet, dvs ett täcknamn för identiteten och sedan kopplas "identitet = pseudonym" ihop i en tabell. Tillgång till tabellen (nyckeln) innebär att det även finns tillgång till informationen om vilken identitet som döljer sig bakom pseudonymen. Detta är en vanlig metod i forskningssammanhang.



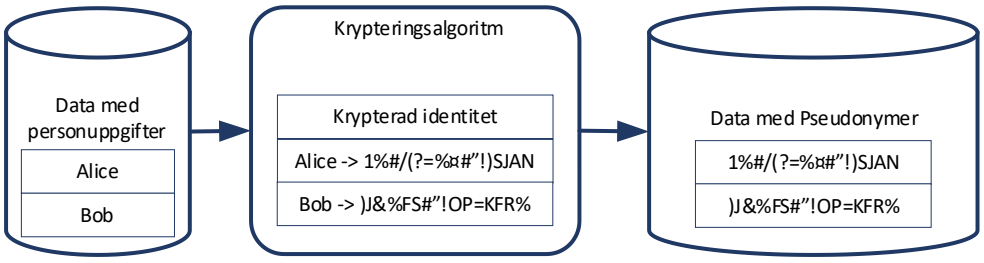
Fördelar med denna metod är att:

- Pseudonymen i sig självt är inte återläsbar till sin ursprungliga identitet
- Det är enklare att lagra ett visst önskat format på en pseudonym
- Säkerhet och behörighetsskydd följer normala koncept för system och applikationer

Det är viktigt att skydda översättningstabellen på ett ändamålsenligt sätt och att ha kontroll på vilka system eller parter som har tillgång till översättningstabellen.

4.3.1.2 Krypteringsalgoritm

En annan metod är att med hjälp av kryptoalgoritmer kryptera den ursprungliga identiteten så den krypterade strängen utgör pseudonymen. Finns tillgång till rätt nyckel kan pseudonymen återläsas till dess ursprungliga identitet.



Krypteringsteknik är i sig ett eget stort teknikområde. Det finns mängder med algoritmer och metoder för att erhålla varierande styrkor på krypton. Generellt sett går det åt mer datakraft ju mer avancerat kryptot är. Den krypterade strängen blir längre ju säkrare kryptering man använder sig av.

Nedan beskrivs två krypteringsmetoder och de grundläggande skillnaderna mellan dessa.

Symmetrisk kryptering
Samma nyckel används för både kryptering samt dekryptering. Nyckeln kan kopieras och distribueras till de som ska ha tillgång till den. Dock innebär det att alla som är innehavare av nyckeln både kan skapa nya pseudonymer och återläsa en krypterad identitet (pseudonym) till dess ursprungliga identitet.

Asymmetrisk kryptering
I detta fall används en publik nyckel för att skapa pseudonymer och en privat nyckel för dekryptering. På så sätt kan de olika nycklarna hållas separerade vilket bidrar till ökad säkerhet. Det öppnar även för en hel del intressanta scenarier där publika nycklar exempelvis kan distribueras till olika organisationer för att skapa pseudonymer medan den privata nyckeln hålls i en annan organisation.

Fördelar med metoden med kodnycklar är:

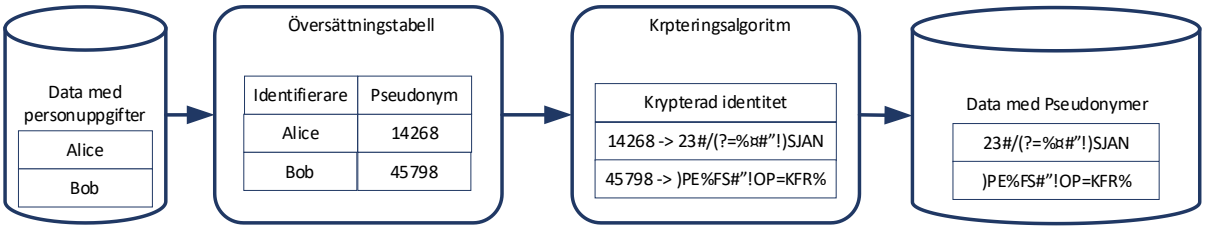
- Att ett register inte behöver hållas
- Det är enkelt att distribuera mellan organisationer
- Asymmetrisk kryptering kan ge säkerhetsmässiga fördelar vid distribuerade lösningar

Nackdelar med metoden är:

- Krypteringar som idag anses starka kanske inte är det om 5-10 år så det bör övervägas vilka risker det kan innebära.
- Den kräver tillit avseende vem som har tillgång till nycklarna.
- Säkerhetsskydd för dessa nycklar kan kräva mer speciell mjuk- och hårdvara.
- Det är svårt att hålla ett speciellt format då dessa pseudonymsträngar kan bli ganska långa och inte följer ett visst format.

4.3.1.3 Kombinerade pseudonymiseringsmetoder

Om behov finns går det även att kombinera olika pseudonymiseringsmetoder. Det går t.ex. att förse en ursprunglig identitet med en pseudonym i en översättningstabell "identitet=123456". När identiteterna ska ersättas i en informationsmängd så identifieras först rätt pseudonym för den identiteten som sedan krypteras med en nyckel.



För att i exemplet kunna återställa ursprungsidentiteten behövs

- Tillgång till nyckeln med krypteringalgoritm för att återläsa pseudonymen
- Tillgång till översättningstabellen för att återläsa den ursprungliga identiteten med ledning av pseudonymen

Fördelarna är primärt säkerhetsmässiga då det krävs tillgång till flera delar som dessutom kan vara separat skyddade för att kunna återläsa den ursprungliga identiteten. Nackdelen är att komplexiteten ökar när flera pseudonymiseringsmetoder kombineras så det bör föreligga starka skäl för att kombinera metoder.

Metoder kan kombineras på olika sätt. Ett alternativ till ovanstående förfarande att först göra en kryptering av identiteten för att sedan göra en översättningtabell. Med ett sådant förfarande erhålls fördelen med krypteringen samt att formatet på psedonymen blir kortare.

4.3.2 Pseudonymisering

När pseudonymiseringen genomförs enligt vald metod skapas pseudonymer kopplade till grundidentiteterna.

Beroende på vilken typ av pseudonymiseringsmetod man väljer så kan pesudonymiseringen vara delad och distribuerad, exempelvis om metoden bygger på asymmetrisk kryptering där en nyckel används för att skapa pseudonymer medan en annan nyckel används för att dekryptera befintliga pseudonymer till dess ursprungsidentitet.

Det är viktigt med rätt säkerhet och skydd för pesudonymiseringen och dess beståndsdelar. Det får inte finnas risk att vem som helst kan komma åt pseudonymerna eller att det uppstår risk för informationsförlust (att t.ex. nyckeln försvinner eller manipuleras). Vid pseudonymisering behöver lämplig säkerhet och skydd övervägas särskilt med hänsyn till skydd för pseudonymiseringens beståndsdelar. Risken för att det skulle kunna skapas en parallell nyckel genom att tillgång getts till både datat med grundidentiteter och det pseudonymiserade datat behöver också beaktas.

4.3.2.1 Pseudonymens format

När man skapar pseudonymer behöver man fråga sig följande:

- Måste pseudonymen strikt följa grundidentitens format?
- Får pseudonymen under inga förhållanden krocka med en redan existerande grundidentitet trots att man vet att det är en pseudonym?
- Medger grundidentitens format utrymme att skapa tillräckligt många unika pseudonymer speciellt om svaret på föregående punkt är nej?

Man bör generellt undvika att använda verksamhetsdata i nyckeln.

En typiskt svår identitet är personnummer där det finns ett förhållandevis litet utrymme för att generera nya unika identiteter om man strikt behöver förhålla sig till personumrets uppbyggnad och format.

4.3.3 Livscykelhantering

När man använder sig av en pseudonymisering så kommer det i de flesta scenarier att innebära att pseudonymer lagras i en datamängd. Därför kan det vara viktigt att dokumentera genomförandet av pseudonymiseringen så att det är möjligt, för det fall det kan behövas, att lösa upp pseudonymen mot en grundidentitet igen.

Det kan också behövas en livscykelhantering av själva pseudonymerna. Det kan handla om tid eller förändrad status på grundidentieten som gör att man kanske vill gallra pseudonymens koppling till grundidentiteten alternativt arkivera denna. Baserat på behoven kan det vara viktigt att ha en förmåga att under hela livscykeln:

- kunna hålla koppling mellan identitet och pseudonym
- kunna svara på frågan; vilken pseudonym har denna identitet
- kunna svara på frågan; vilken identitet har denna pseudonym
- kunna ta bort kopplingen mellan identitet och pseudonym

För att stödja livscykelhanteringen för pseudonymer kan följande information vara av vikt.

- Tidsstämplar per pseudonym för händelser, exempelvis “skapad, uppdaterad”
- Information om själva pseudonymiseringen, denna information bör dock inte spridas till obehöriga
    - Unik identitet
    - Identitetstyp “exempelvis personnummer, regnr”
    - Ägarskap

- Tidsstämplar och status

Om man har behov av att med jämna mellanrum förnya pseudonymer för en grundidentitet kan man göra det på lite olika sätt. Vill man använda samma pseudonymisering för detta går det att addera funktionalitet och hålla en historik av pseudonymer och även status för dessa, exempelvis "aktiv, inaktiv, gallrad".

Ett annat sätt att åstadkomma detta är att sätta upp en ny aktiv pseudonymisering som skapar nya pseudonymer för grundidentiteterna.

5. Användningsområden och möjligheter med pseudonymisering

5.1 Exempel på scenarier med pseudonymisering

Det finns olika scenarier där det kan vara aktuellt att överväga att tillämpa pseudonymisering, t.ex.

- Ökade säkerhetskrav – spårbarhet och loggning
- I utvecklingsarbetet – att kunna testa lösningar
- Kombinera data från olika källor
- Användning av molntjänster
- Minska risker vid personuppgiftshanteringen inom en organisation och vid utkontraktering
- Enkäter

Nedan ges en beskrivning av några sådana scenarier. Samtliga scenarier förutsätter att det finns en rättslig grund för att behandla personuppgifterna i detta syfte och att andra dataskyddsrättsliga eller förvaltningsrättsliga krav (såsom sekretess) har beaktats.

5.2 Ökad säkerhet för personuppgiftsbehandlingen internt inom en offentlig organisation

5.2.1 Hantering av personuppgifter inom en organisation för användning i loggsystem

Scenariot utgår ifrån ett behov av att ersätta grundidentiteterna med pseudonymer innan data förs över till annan del inom organisationen. Det skulle t.ex. kunna vara en tänkt lösning för överföring av data ett loggsystem.

5.2.2 Pseudonymisering av handläggares identitet

Detta scenario utgår från ett behov av att skydda handläggarens identitet vid handläggning av känsliga ärenden, exempelvis vid utmätningar av fastigheter, socialtjänstärenden och domstolsärenden. Vid handläggning av ett ärende sparas en pseudonym för handläggaren istället för dennes riktiga identitet. Om syfte, behörighet och lagstiftning kräver det så går det att återläsa pseudonymen till dess grundidentitet. Vem som har gjort återläsningen och när det gjordes bör loggas.

5.2.3 Pseudonymisering av sökandes identitet vid ärendehandläggning

Detta scenario utgår från att det vid vissa handläggningar av ärenden eller ansökningar inte finns behov av att handläggaren ska känna till grundidentiteten för den sökande eller den person handläggningen gäller. Motivet här kan vara att minska hanteringen av personuppgifter i klartext. I sådana fall kan grundidentiteten ersättas med en pseudonym i handläggningsgränssnittet så att den faktiska identiteten förblir okänd för handläggaren.

Om syfte, behov och behörighet finns kan en funktion erbjudas för att låsa upp pseudonymen till dess grundidentitet.

5.2.4 Pseudonymisering av skyddade identiteter

Detta scenario utgår från att hantera personuppgifter vars identitet på olika sätt är skyddad. Hanteringen av skyddade personuppgifter är komplex. I en lösning för att hantera skyddade personuppgifter kan pseudonymisering utgöra en viktig beståndsdel.

5.2.5 Använda pseudonymiserad information för att träna AI-modeller

Detta scenario utgår från ett behov av att träna en AI-modell (artificiell intelligens) vars syfte är att ge stöd vid tillämpningar så som ärendehandläggning, brottsförebyggande arbete etc. När AI-modellen tränas kan skäl för att använda produktionsdata vara att få en så realistisk hantering som möjligt. Samtidigt kan det finnas skäl att begränsa risken med personuppgiftshanteringen genom att pseudonymisera grundidentiteterna. Efter det att övningsdatat framställts kan referensen mellan grundidentiteteteterna och pseudonymerna tas bort. Om referensen tas bor tas möjligheten att addera mer övningsdata med bibehållna pseudonymer bort.

I scenariot behöver det särskilt övervägas om det finns risk för att träningen försämras om pseudonymiserade uppgifter används och om detta är en rimlig effektförlust utifrån syftet med behandlingen.

Motsvarande förfarande kan användas för att producera och använda testdata i olika typer av tillämpningar där det är lämpligt.

5.3 Ökad säkerhet för personuppgiftsbehandlingen i relationen med aktörer utanför den egna organisationen

5.3.1 Pseudonymer vid nyttjande av externa tjänster

Detta scenario utgår från att det används en extern tjänst för sina anställda dit inloggning kan ske med med en pseudonym i stället för den anställdes identitet. På så sätt minskas exponeringen av de interna identiteterna till externa tjänsteleverantörer.

Scenariot fungerar på enklare externa tjänster som inte kräver ytterligare lagring av personuppgifter i tjänsten alternativt tjänster som är anpassade för pseudonymer och lagring av personuppgifter utanför tjänsten.

Vissa inloggningstjänster kräver tvåstegsautentisering där någon del kräver personlig identifiering. I sådana fall är pseudonymisering inte en tillämpbar åtgärd.

5.3.2 Hantering av personuppgifter som kan låsas upp av mottagaren baserat på syfte

Detta scenario utgår ifrån ett behov av att ersätta grundidentiteterna med pseudonymer innan data förs över till en annan organisation.

Mottagande organisation ser sedan anledning till att återläsa grundidentiteten för en viss pseudonym vilket utförs genom att den sändande organisationen bistår i översättning till grundidentiteten. Syfte och rättigheter avgör om det finns stöd för att återläsa pseudonymernas grundidentitet. Det skulle t.ex. kunna vara att en myndighet i ett första steg erhåller pseudonymiserade uppgifter för att göra en analys för att förhindra felaktiga utbetalningar. Om analysen påvisar ett intressant mönster kan som ett nästa steg nyckeln lämnas över så att den mottagande myndigheten kan låsa upp det pseudonymiserade materialet om rättsliga förutsättningar föreligger för detta.

5.3.3 Användning av pseudonymiserade uppgifter i forskningssyfte

I detta scenario lämnar en organisation (A), eller flera organisationer (A och B), data som innehåller grundidentiteter till organisationen C. Organisationen C pseudonymiserar uppgifterna och förmedlar dessa till extern part i forskningssyfte. Exempelvis kan uppgifter som Skatteverket och Arbetsförmedlingen lämnar till Statistiska Centralbyrån pseudonymiseras hos Statistiska centralbyrån och lämnas ut till en extern aktör i forskningssyfte. I vissa fall kan scenariot också innebära att C lämnar ut nyckeln till

organisation D som använder samma pseudonym för sin data och skickar pseudonymiserade uppgifter till samma forskningsprojekt.

Scenariot förutsätter att organisation A och B har rätt att överföra data som innehåller grundidentiteter till organisation C. Därtill behöver organisation C ha en rättslig grund för att behandla och pseudonymisera uppgifterna och också få lämna ut dessa i forskningssyfte. Rättslig grund behövs för varje behandlingssteg i processen.

5.3.4 Analys av pseudonymiserad information från flera organisationer

I vissa fall finns ett behov av att kunna sambearbeta stora mängder data från olika källor. Sådana behov framförs särskilt när det gäller digitalisering av verksamhetsprocesser, analyser och användning av applikationer inom artificiell intelligens (AI) eller stordata (Big Data).

Detta scenario utgår från ett behov av att analysera data innehållande personuppgifter från flera organisationer. Syftet med bearbetningen är att erhålla bättre kunskap och insikter om samband mellan olika datamängder vilket i ett senare skede kan leda till verksamhetsförbättringar. Själva personuppgiften och individen i sig är inte intressant, däremot har man behov av att veta att det är samma identitet som står bakom olika uppgifter eller händelser i den datamängden för att analysen ska ge önskat värde. Det behövs således en koordinerad pseudonymisering.

I scenariot överför organisation A, B och C data till organisation D. Personuppgifterna i det överförda datat pseudonymiseras innan behandling sker hos organsiation D. Pseudonymiseringen görs i detta exempel av en fristående enhet. Men det skulle också vara möjligt att pseudonymiseringen sker hos A, B och C, men att det då ändå behöver vara koordinerad. Organisation D kan antingen utföra analys för egen räkning eller genomföra analys för A, B och Cs räkning.

Det kan föreligga rättsliga utmaningar för sådan behandling. Det kan vara svårare för A, B och C att hitta en rättslig grund för att lämna data som innehåller grundidentiteter till pseudonymiseringsenheten och grund för att uppgifterna får behandlas på detta sätt. Syftet med behandlingen måste enligt dataskyddsbestämmelserna vara tydligt för att behandling ska få ske och ofta finns det begränsningar i för vilka nya syften uppgifterna får behandlas (finalitetsprincipen). Det kan också uppstå frågor kring s.k. gemensamt personuppgiftsansvar för behandlingen.

5.4 Utökade möjligheter att utbyta information mellan aktörer

Ett scenario som ofta efterfrågas är om data som innehåller grundidentiteter eller pseudonymiserade uppgifter kan anonymiseras och därmed inte längre utgör personuppgifter. Behandling skulle då vara möjlig utan att beakta dataskyddsbestämmelserna, vilket sannolikt skulle öppna upp för nya möjligheter att behandla uppgifterna, t.ex. genom stordataanalys. Scenariot kan vara att organisation A pseudonymiserar uppgifter och lämnar till organisation B eller att det är fråga om en kedja där A pseudonymiserar och lämnar till B som i sin tur bearbetar uppgifterna och lämnar till C.

Det är svårbedömt när en anonymisering kan anses ha uppnåtts, se avsnitt 3.1.2 och 6. Denna vägledning har avgränsats till att omfatta användning av pseudonymisering och innehåller inte några överväganden kring anonymisering. Men området är intressant för offentlig verksamhet att utforska vidare.

6. Faktiska exempel på användning av pseudonymisering

I detta avsnitt redovisas några faktiska exempel på hur pseudonymisering används inom offentlig verksamhet, där några myndigheter bidragit med sina erfarenheter.

6.1 Pseudonymisering för obligatorisk kontroll av licens hos extern leverantör

Lantmäteriet använder sig av ett kontorsstöd från en leverantör som i sitt avtal för licenshantering kräver att varje användare har ett eget konto för att verifiera den personliga licensen. För att undvika att persondata delas till leverantören har Lantmäteriet pseudonymiserat samtliga användarkonton så att varken namn, mailadress eller andra personuppgifter är kända för leverantören.

Lösningen bygger på en lokal installation av kontorssviten och att all användning av programvaran sker lokalt inom Lantmäteriet. Utbytet av kontoinformation används enbart för att uppfylla leverantörens licensieringskrav.

6.2 Skapa möjlighet till analys av stora datamängder

Sveriges Kommuner och Regioner (SKR) har på uppdrag av regionerna utrett hantering av patientrapporterade data. Pseudonymisering kan ske på många sätt, men utredningens förslag är att skapa en metod för så effektiv och säker pseudonymisering som möjligt. Metoden innebär att data som beställs för konsumtion från en lagringsplats först separeras i olika delar, där en del innehåller den känsliga informationen. Data mellanlandar, och byts ut mot oigenkännliga data, hos en extern säkerhetsleverantör. Därefter skickas den vidare till konsumenten där datamängden paras ihop igen med de övriga datadelarna som hade beställts.

Processen följer infrastrukturen för PKI (public key infrastructure), infrastruktur för kryptering med öppen nyckel (asymmetrisk kryptering). PKI är ett system som, med användning av elektroniska certifikat, gör det möjligt att kontrollera att en viss publik nyckel verkligen tillhör den påstådda ägaren. PKI förutsätter att det finns certifikatutfärdare som både utfärdar certifikat, och som kan återkalla dem vid behov. Förutom att data förblir krypterat i hela processen så sker även en så kallad hashning[30]

[30] Del av pseudonymiseringsmetoden med krypteringsalgoritm.

som ersätter eventuell känslig personinformation i den data som hämtas, med en icke identifierbar kod, innan informationen kommer fram till mottagaren.

I patientrapporterade data finns det framför allt ett attribut som är att betrakta som känslig personinformation, nämligen personnummer. Teoretiskt skulle man kunna ta bort personnummer helt, men då försvinner också viktig bakgrundsinformation som behövs vid analys- och statistikbearbetning. För att kunna dra meningsfulla slutsatser vill man gärna veta ålder och kön på patienter som svarar på enkäter och de variablerna läses ut från personnumret. En möjlighet är då att ta fram de variablerna ur ett personnummer och skicka endast dem vidare tillsammans med enkätsvaren till mottagaren. Då finns dock ingen möjlighet att återskapa personinformationen vilket kan vara viktigt för t.ex. forskning i framtiden. En annan anledning till att man gärna vill kunna identifiera vilken svarsdata som tillhör en viss patient är om det finns anledning att para ihop den informationen med data om samma patient från andra datakällor.

Lösningen är således hashning med en krypteringsstandard som heter SHA-2 (Secure Hash Algorithm 2). Processen ersätter personnumret med en krypterad kod som skapas med utgångspunkt i en kombination av vårdgivarens organisationsnummer (förslagsvis HSAID) och patientens personnummer.

Säkerhetsprocessen är inspirerad av en amerikansk lösning på ett lagkrav som beslutades år 2014 i Massachusetts (Chapter 55 of the Acts of 2014).

Lagen krävde att staten skulle skapa analysunderlag avseende de dödsfall som skett med opioider under året. Informationen fick under inga omständigheter vara personidentifierande. För att få till ett adekvat analysunderlag insåg man att datakällor från flera dataägare behövde kopplas ihop. För att det skulle vara möjligt utan att använda personidentifierande information, som parningsnyckel, konstruerades en avancerad datautbytesprocess. Därefter kunde man slå ihop olika typer av information från olika datakällor och samtidigt vara säker på att de på radnivå tillhörde samma individ. I målkällan fanns ingen personligt identifierbar information kvar utan den befanns sig fysiskt på en helt annan plats.

Chapter 55-förfarandet liknar på många sätt den lösning som utredningen beskriver. En intressant skillnad är dock att istället för att information överfördes via säkra API:er mellan datakällor, så sparades den ner på USB-minnen som helt enkelt budades över till målkällan.

6.3 Pseudonymisering vid digital identitet, EFOS

Försäkringskassan ansvarar för en gemensam tjänst för att hantera e-identiteter för offentlig sektor (EFOS). Bakgrunden till skapandet av en gemensam tjänst var att generaldirektörerna för Arbetsförmedlingen, Försäkringskassan och Skatteverket i september 2007 skrev under ett avtal om samverkan mellan myndigheter inom området. Lösningen möjliggör för myndigheter att ha en gemensam lösning kring e-tjänstelegitimationer. Just nu används tjänsten bl.a. av Barnombudsmannen, Brottsoffermyndigheten, Försäkringskassan, Kronofogdemyndigheten, Myndigheten för digital förvaltning, Pensionsmyndigheten, Riksgälden, Skatteverket, Statens Servicecenter och Tullverket.

Medarbetare inom EFOS behöver kunna identifiera sig inte bara internt utan även externt, både inom Sverige och utomlands. EFOS tillhandahåller e-tjänstelegitimationer och använder sig av personnummer för identifiering och i underskriftscertifikatet har personnummer ersatts med EFOS ID, som är en unik identitet inom EFOS. EFOS ID är en pseudonym för grundidentiteten.

De tjänster som använder EFOS för identifiering har olika krav på identifiering. Vissa kan använda sig av grundidentiteten och vissa av pseudonymen som utgörs av EFOS ID. Ännu finns inga offentliga tjänster som tar emot pseudonym. När tjänsterna är anpassade för det kommer EFOS att nyttja EFOS ID i dessa.

6.4 Pseudonymisering i relationen till en extern leverantör

Skolverket har i uppdrag från regeringen att utveckla och tillhandahålla digitaliserade nationella prov och bedömningsstöd i grundskolan och på gymnasial nivå. En så stor andel av proven som möjligt ska automaträttas (se U2017/03739, U2019/03788).

Arbetet har pågått sedan 2017 då även upphandlingen av it-lösningen för digitaliserade prov inleddes. Under samma tidsperiod som upphandlingen genomfödes blev frågan om tredjelandsöverföringar av personuppgifter aktualiserad inom Sverige. Skolverkets leverantör hade en ägarstruktur som gjorde att tredjelandsöverföring blev en fråga som behövde hanteras och olika handlingsalternativ analyserades. Ett av alternativen omfattade att pseudonymisera personuppgifterna i it-lösningen.

6.4.1 Utformning av it-lösningen

Den upphandlade it-lösningen ska hantera personuppgifter kring t.ex. elever, lärare och andra roller som ingår i it-systemet. Skolverket skissade på en lösning som skulle innebära att endast pseudonymiserade uppgifter om personer hanterades i it-lösningen.

Detta skulle innebära att kringliggande lösningar behövde etableras för att hantera översättningar mellan personuppgifter och de pseudonymer som ersätter identiteter.

6.4.2 Skolverket arbete med pseudonymisering

I Skolverkets fall, i arbetet med digitaliseringen av de nationella proven, handlade det om att personuppgifter för hundratusentals användare skulle behandlas i ett system där driften omhändertogs av en stor och etablerad internationell molntjänstleverantör. Genom Schrems II-domen har EU-domstolen tydliggjort att det kan krävas kompletterande åtgärder för att överföra personuppgifter till tredje land. Så är fallet om mottagarlandet inte kan anses tillförsäkra en i allt väsentligt likvärdig skyddsnivå för uppgifterna som inom EU och EES. Skolverket kunde utifrån domen konstatera att det är svårt att åstadkomma en laglig hantering av personuppgifter i molntjänster med ägande utanför EU och EES eftersom det ofta då finns en hantering eller risk för en potentiell hantering av uppgifterna i tredjeland i strid med dataskyddsförordningen.

Skolverket utvärderade den uppkomna situationen för att komma fram till den optimala lösningen på utmaningarna som Schrems II-domen gav upphov till för myndigheten. Pseudonymisering utvärderades som en potentiell kompletterade skyddsåtgärd men det stod klart att en sådan lösning skulle vara svår att genomföra och riskfylld ur juridiska, prestanda- och säkerhetsaspekter. Skolverket bestämde istället att flytta hela provtjänsten och behandlingen till en EU-baserad molntjänst som möjliggör efterlevnad av GDPR.

6.4.3 Kontentan – vad Skolverket har kommit fram till

Pseudonymisering kan vara en bra metod att använda som kompletterande skyddsåtgärd i vissa fall, exempel kan vara i statistik, rapporter eller underlag för beslut. För molntjänster där run time-miljön kräver ständig pseudonymisering eller de-pseudonymisering för att verksamhetskraven ska uppfyllas är det dock utmanande att få att fungera. När ständig de-pseudonymisering krävs som i den provtjänst som var aktuell i det här fallet kan det medföra utökad komplexitet till den grad att behandlingen blir omöjlig och att pseudonymiseringen inte blir genomförbar. Risker för dålig prestanda, höga kostnader och svårigheter i förvaltningen är uppenbara.

En bättre lösning är att försöka utföra behandlingen av personuppgifter i en miljö som är kompatibel med gällande lagar och bestämmelser. Sedan kan pseudonymisering tillämpas i denna miljö vid behov.

6.5 Pseudonymisering på SCB

Inom SCB används begreppet kodnyckel för det som i denna vägledning beskrivs som översättningstabell i avsnitt 4.3.1.1.

6.5.1 Utlämnande

Enligt SCBs Sekretesspolicy ska utlämnande av uppgifter som är direkt hänförliga till en enskild ske mycket restriktivt. I uppdrag där uppgifterna behövs för forskning lämnar SCB, i dialog med mottagaren, som regel endast ut uppgifter som inte är direkt hänförliga till en enskild. De identifierbara uppgifterna ersätts då med ett unikt löpnummer.

När SCB lämnar ut uppgifter som inte direkt kan hänföras till en enskild får uppgifterna, enligt 16 § lagen (2001:99) om den officiella statistiken, förses med en unik beteckning, som kan kopplas till ett personnummer eller motsvarande med hjälp av en kodnyckel som bevaras hos SCB under en längre tid. De uppgifter som lämnas ut kan då kompletteras såväl med nya årgångar som med nya uppgifter och även utökade populationer. En kodnyckel får dock bara användas för att komplettera och uppdatera material i ett visst forsknings- eller statistikprojekt.

Den praktiska hanteringen i punktform:

- Löpnumren som ersätter identiteter är helt informationslösa.
- Den aktuella populationen sorteras slumpmässigt och numreras sedan från 1 till n.
- Samma löpnummer används genomgående för samma identitet.
- Vid en utökning fortsätter numreringen från det högsta använda talet.
- Varje uppdrag har en unik kodnyckel.

6.5.2 Användning av kodnyckeln

En hantering med kodnycklar är möjlig vid utlämnande av uppgifter till andra myndigheter och till fysiska och juridiska personer. En kodnyckel får dock bara användas för att komplettera och uppdatera material i ett visst forsknings- eller statistikprojekt. Det innebär att kodnyckeln inte får användas för att senare lämna ut uppgifter till andra mottagare eller för andra projekt än det som nyckeln skapades för. När det ursprungliga projektet har upphört saknas förutsättningar för att bevara kodnyckeln.

6.5.3 Bevarandetid för kodnyckeln

I samband med beslut om utlämnanden av uppgifter fattas beslut om kodnyckelns bevarande.

Stöd för bevarande måste finnas i exempelvis forskningsplan eller etikansökan. Innan bevarandetiden för nyckeln går ut kan projektet ansöka om förlängning, om stöd för detta finns. Det finns en dom från Förvaltningsrätten i Karlstad som avser bevarande av kodnycklar till forskningsdatabaser (mål nr 2874–20).

7. Rekommendationer

För att avgöra om pseudonymisering kan vara aktuellt krävs inledningsvis en bedömning om de aktuella uppgifterna utgör personuppgifter enligt definitionen i dataskyddsförordningen (se avsnitt 2.1.1). Domen i Breyer-målet kan vara ett stöd i den bedömningen (se avsnitt 3.1.2).

7.1 Rekommendationer inför en pseudonymisering

I denna vägledning har inte ingått att närmare analysera förutsättningar för anonymisering och när sådan uppnås, men det kan konstateras att kraven för att uppnå en anonymisering är höga. Många gånger kommer det gå att härleda uppgifterna bakåt så länge data som innehåller grundidentiteter finns kvar.

Inom en verksamhet är det svårt att anonymisera personuppgifter då organisationen är personuppgiftsansvarig och således har tillgång till uppgifterna även om åtkomsten till dem internt har avgränsats med behörigheter. Vid överföring av uppgifter från en organisation till en annan (och även vidare till en tredje organisation) skulle det kunna vara möjligt att åstadkomma en anonymisering om det föreligger ett förbud för mottagande part att ta del av data som innehåller grundidentiteter eller kompletterande uppgifter eller om det bedöms som orimligt utifrån tillgängliga resurser.

Vad som är ”orimligt utifrån tillgängliga resurser” är svårbedömt och risken finns att anonymiserade uppgifter med nyare teknik kan komma att kunna knytas till en viss person. En myndighet bör noga överväga syftet med att behandla personuppgifterna på det sätt man önskar göra. Man måste också bedöma om det är möjligt att genomföra med en pseudonymisering (där uppgifterna fortfarande utgör personuppgifter och måste behandlas i enlighet med dataskyddsregelverket). Att behandlingen ryms inom myndighetens uppdrag är centralt i sammanhanget.

Genom en pseudonymisering kan risker med behandlingen av personuppgifterna minskas. Inför en pseudonymisering kan det därför vara bra att utgå från ett önskat scenario utan pseudonymisering och identifiera vilka hinder eller risker som föreligger. Därefter kan undersökas som en pseudonymisering kan bidra till att minska dessa hinder eller risker till en acceptabel nivå som gör att behandlingen bedöms möjlig att genomföra.

I vissa fall är pseudonymisering en mindre lämplig metod, såsom när det i något skede finns ett behov av att veta vem som agerat eller utfört en viss åtgärd. Det bör därför inför en pseudonymisering undersökas om uppgifterna kommer att behövas i klartext i

något skede i processen och utifrån det avgöras om pseudonymisering är lämpligt eller inte.

Beträffande externa molntjänster finns sannolikt begränsade förutsättningar att använda sig av pseudonymisering. Skälen till det är flera. Vilka förutsättningar som finns för pseudonymisering beror på vad det är för typ av personuppgifter som hanteras i tjänsten och i vilken omfattning samt vad tjänsten syftar till (funktionalitet m.m.). Många gånger behöver uppgifter hanteras i klartext, t.ex. att deltagare behöver veta eller se vem de kommunicerar med. De användningsfall som nämns i EPDBs rekommendationer[31] tar sikte på att skicka personuppgifter till tredjeland för analysändamål. Användningsfallet som rör kryptering gäller endast lagring av personuppgifter. Vid bedömning av om pseudonymisering är en lämplig eller möjlig åtgärd bör man beakta uppgiftsmängden och grad av komplexitet.

Om man behandlar uppgifter om individer och har en extern leverantör av ett it-system för att stödja verksamheten är det inte lämpligt att använda pseudonymer om stöd för detta inte finns inbyggt i it-stödet hos leverantören. Att påföra pseudonymiseringsfunktioner utanför it-stödet kan med stor sannolikhet bli komplext.

Som framgått ovan kan de kompletterande uppgifterna många gånger bedömas utgöra en allmän handling. Innan man tar ställning till pseudonymisering bör det därför övervägas under vilka förutsättningar de kompletterande uppgifterna skyddas.

7.2 Rekommendationer vid genomförande av en pseudonymisering

Vid införandet av pseudonymisering kan det behöva göras en avvägning mellan risk och nytta och om värdet (för den enskilde respektive organisationen) med behandlingen går förlorat om en pseudonymisering genomförs. Det behöver göras en riskanalys.

Vid en pseudonymisering bör noga övervägas vilken metod som är mest lämplig att tillämpa, utifrån syftet med pseudonymiseringen, vilken behandling som ska göras med uppgifterna och tillhandahållandesätt. För val av lämplig pseudonymiseringsmetod behöver också krav på skalbarhet och prestanda definieras.

Premisserna för den tekniska miljön behöver säkerställas. Det är viktigt med rätt säkerhet och skalskydd med begränsade behörigheter så att inte vem som helst kan komma åt pseudonymerna eller att det uppstår risk för informationförlust (att t.ex. nyckeln

[31] Europeiska dataskyddsstyrelsens (EDPB:s) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

försvinner eller manipuleras). Vid pseudonymisering behöver lämplig säkerhet och skydd övervägas särskilt med hänsyn till skydd av de kompletterande uppgifterna.

Det är viktigt att avgöra vem som har rättighet och behörighet att hantera pseudonymen, såsom vem som har åtkomst till översättningstabell eller kodnyckel och vem som får återläsa en pseudonym till dess ursprungliga identitet.

Skapandet av pseudonymer och hanteringen av lösningen behöver tänkas igenom utifrån ett livcykelperspektiv, bl.a. utifrån spårbarhet och regler för arkivering och gallring. Det är viktigt att dokumentera hur pseudonymiseringen är utformad och vilken pseudonymiseringsenhet som skapat en pseudonym i en viss datamängd i det fall behov finns av att kunna lösa upp pseudonymen mot en grundidentitet igen. Även dokumentation som beskriver lösningen behöver skyddas med lämplig säkerhetsnivå.

Det kan finnas behov av att upprätta avtal, t.ex. personuppgiftsbiträdesavtal, i de fall flera parter är inblandade.

8. Checklista för pseudonymisering

.

	Inför en pseudonymisering
1	Vad är syftet med pseudonymiseringen? Vad ska uppnås? Vilka behov ska lösas?
2	Finns det en rättslig grund för sådant syfte och behandling i myndighetens uppdrag?
3	Vilken datamängd är tänkt att pseudonymiseras?
4	Innehåller datamängden som ska behandlas personuppgifter? Om inte faller hanteringen utanför dataskyddsregelverket.
5	Är det möjligt att helt göra den registrerade oidentifierbar? I sådana fall finns förutsättningar för att anonymisera annars är det fråga om pseudonymisering.
6	Är pseudonymisering ett lämpligt verktyg? • Kommer de kompletterande uppgifterna anses vara allmänna handlingar? Om ja, bedöms de kompletterande uppgifterna skyddas av sekretess? Om nej, pseudonymisering är inget bra alternativ, om ja, pseudonymisera. • Behövs uppgifterna i klartext? Om ja är inte pseudonymisering ett gångbart alternativ. • Föreligger hög komplexitetsgrad? Om ja kan pseudonymisering vara en mindre lämplig metod.

	Genomförande av en pseudonymisering
1	Är det tydligt vem (vilka roller) som är ansvarig för de olika delarna av pseudonymiseringen?
2	Har informationsklassning och riskanalys genomförts?

3	Hur säkerställs principerna och övriga krav enligt dataskyddsregelverket? Behöver konsekvensbedömning genomföras?
4	Behövs ytterligare tekniska och organisatoriska åtgärder för att säkerställa efterlevnaden av dataskyddsregleringen (loggning, behörighetsstyrning m.m.)
5	Hur hanteras de kompletternade uppgifterna? (Lagringsyta, när sker gallring osv.)
6	Har övervägande gjorts om val av metod? Varför har en specifik metod valts?
7	Vilka krav finns på utformning av pseudonym? • Måste pseudonymen strikt följa grundidentitens format? • Får pseudonymen under inga förhållanden krocka med en redan existerande grundidentitet trots att man vet att det är en pseudonym? • Medger grundidentitens format utrymme att skapa tillräckligt många unika pseudonymer speciellt om svaret på föregående punkt är nej?
8	Är tekniska och säkerhetsmässiga förutsättningar omhändertagna?
9	Har dokumentation av pseudonymiseringen för ett livcykelperspektiv omhändertagits?

eSam är ett medlemsdrivet program för samverkan mellan myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälso-myndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet.