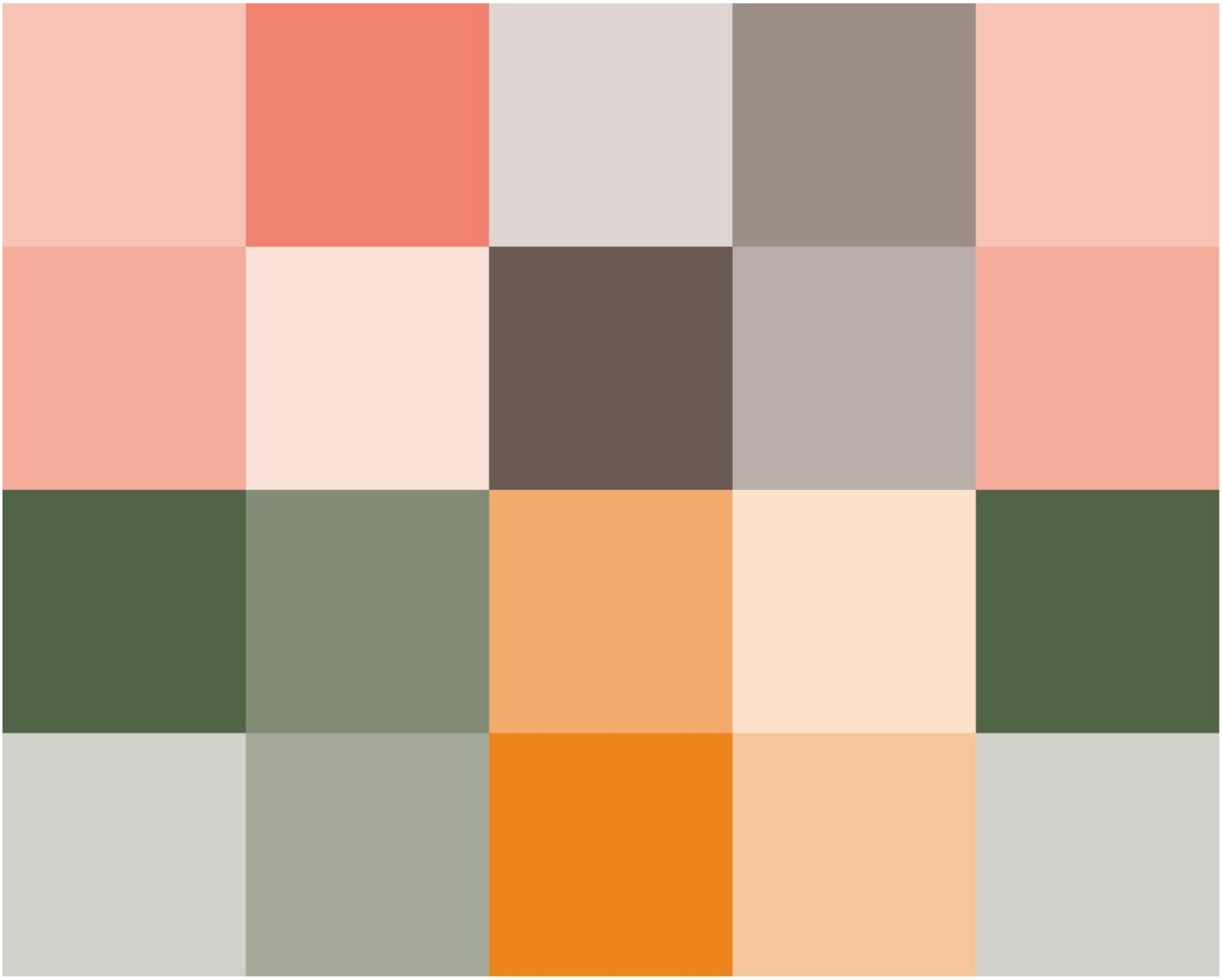

Bilaga 3, Juridiska problemställningar

I2021/01595

2021–12–15

DIGGs ärendenummer: 2021-1342

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1 Inledning

Det tekniska systemet för bevisutbyte väcker flera juridiska problemställningar som måste hanteras utifrån svensk rätt. Av uppdraget framgår att det ska innehålla en beskrivning och exemplifiering av eventuella förvaltningsgemensamma eller myndighetsspecifika juridiska problemställningar när det gäller det gränsöverskridande bevisutbytet samt eventuella juridiska problemställningar avseende sekretess och personuppgiftsbehandling. De problemställningar som vi inom ramen för detta uppdrag har identifierat är främst att en grundläggande svårighet med bevisutbytet är att det är oklart hur det ska uppfattas utifrån svensk rätt, det vill säga om det ska ses som ett direkt utbyte mellan behöriga myndigheter eller som en överföring av bevis på begäran av den enskilde. Beroende på vilket synsätt som anläggs uppstår vissa juridiska problemställningar utifrån svensk rätt.

Om det tekniska systemet för bevisutbyte ses som ett utbyte direkt mellan myndigheter uppstår en problemställning om hur bevis som innehåller uppgifter som är sekretessreglerade ska hanteras. Sekretess kan gälla gentemot myndigheter eller andra aktörer. Ytterligare juridiska problemställningar, eller snarare risker, är hur det tekniska systemet förhåller sig till GDPR. Dessa frågor, som främst är av förvaltningsgemensam karaktär, kommer vi att närmare behandla i de följande avsnitten. Därefter kommer vi även att behandla identitetsmatchning och juridiska problemställningar kopplade till den frågan. I det avslutande avsnittet kommer myndighetsspecifika problemställningar som främst är kopplade till registerförfattningar att behandlas.

Av artikel 14 (9) i SDG-förordningen fastlås att kommissionen senast den 12 juni 2021 ska anta genomförandeakter för att fastställa de tekniska och operativa specifikationer hos det tekniska systemet som behövs för genomförandet. Dessa genomförandeakter har fortfarande inte antagits. Mot denna bakgrund får vi inom ramen för detta uppdrag göra vissa antaganden kring hur det tekniska systemet kommer att se ut. I den fortsatta framställningen kommer vi därför att beskriva dels de lösningar som Sverige förespråkar, dels de lösningar som kommissionen föreslagit i sitt senaste utkast till genomförandeakt.

Som angetts ovan omfattar uppdraget att beskriva och exemplifiera *förvaltningsgemensamma* juridiska problemställningar. Begreppet *förvaltningsgemensamt* har ingen legaldefinition. I detta uppdrag använder vi oss av den kvalificering och innebörd som DIGG använde sig av i slutrapporten om

etablering av rättsligt stöd (I2021/00288, dnr: 2021–168). *Förvaltningsgemensamt* definieras då bland annat som att det är en fråga som berör flera offentliga aktörer och flera typer av offentliga aktörer.

Likaså när det gäller *myndighetsspecifika* problemställningar har inte det begreppet heller någon legaldefinition. Det har inom ramen för detta uppdrag inte varit möjligt att identifiera någon problemställning som endast berör en enstaka myndighet. Inom ramen för detta uppdrag har vi därför definierat begreppet *myndighetsspecifikt* utifrån att det är en fråga som inte är av generell karaktär och således inte berör alla myndigheter.

2 Överföring av bevis inom bevisutbytet

Det tekniska systemet för bevisutbyte enligt engångsprincipen regleras i artikel 14 i SDG-förordningen. Ett bevis definieras i förordningen som ett dokument eller data, inbegripet text eller ljud, bildinspelningar eller audiovisuella inspelningar, oavsett vilket medium som använts, som en behörig myndighet begär för att bevisa fakta eller överensstämmelse med de formkrav som avses i artikel 2.2 b.[1] De bevis som kommer att överföras inom systemet kommer att variera och kan till exempel vara ett utdrag från folkbokföringen. Det tekniska systemet för bevisutbyte ska enligt artikel 14 (4) endast användas på den enskildes uttryckliga begäran och är alltså inte obligatoriskt.

Det tekniska systemet för bevisutbyte innebär att en behörig myndighet som utfärdar ett visst bevis på begäran ska tillhandahålla beviset inom systemet. Beviset ska överföras till ett utrymme där den enskilde får förhandsgranska beviset och avgöra om denne vill använda beviset i förfarandet. Därefter ska beviset överföras från den tekniska ytan för förhandsgranskning till förfarandet. En grundläggande juridisk svårighet är att det är oklart om det tekniska systemet för bevisutbyte ska uppfattas som att överföringen av bevis sker på den enskildes begäran eller som ett utbyte direkt mellan myndigheter, vilket påverkar efterföljande frågor om

[1] Artikel 3 i SDG-förordningen.

sekretess. Den processuella miljön för förhandsgranskning väcker även juridiska problemställningar avseende hur utrymmet ska hanteras i juridisk mening.

2.1 Utlämnande enligt TF

En handling är enligt tryckfrihetsförordningen (TF) en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.[2] En sådan handling är allmän om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos en myndighet.[3] De bevis som kommer att utbytas i systemet kommer från svensk synvinkel i princip enbart att vara allmänna handlingar. I detta sammanhang ska även nämnas att offentlighetsprincipen, som är definierad i 2 kap. 1 § TF, ger var och en rätt att ta del av allmänna handlingar. En sådan rätt gäller för enskilda medborgare, såväl svenska som utländska.

I det tekniska systemet för bevisutbyte kommer det begärda beviset att exporteras från myndighetens yta till den tekniska ytan för förhandsgranskning. Enligt vår bedömning får överföringen från myndigheten juridiskt sett anses motsvara ett utlämnande enligt TF. Nästa fråga som aktualiseras är på vems initiativ som utlämnandet sker och beroende på vilket som får anses gälla kan vissa juridiska problemställningar uppstå. Ett utlämnande av en handling kan begränsas om uppgifterna omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL), vilket kommer att avhandlas i avsnitt 3.

En juridisk problemställning som anknyter till offentlighetsprincipen kan uppstå när bevis överförs inom bevisutbytet till förfaranden i Sverige. Som huvudregel blir bevis allmänna handlingar när de inkommit till svenska myndigheter. Eftersom det står klart att andra medlemsstater inte i samma utsträckning tillämpar en offentlighetsprincip så som i Sverige kan det uppstå en diskrepans i förhållande till andra medlemsstater. Handlingar som i andra länder som utgångspunkt omfattas av sekretess kan i Sverige begäras ut som allmän handling. Det kan leda till att andra länder uppfattar det som negativt att överföra bevis till förfaranden i Sverige då bevisen som huvudregel blir allmänna handlingar och kan begäras ut av var och en. På sikt kan denna skillnad skada förtroendet för systemet för bevisutbyte och leda till en minskad användning.

[2] 2 kap. 3 § TF.
[3] 2 kap. 4 § TF jämte 9 och 10 §§ TF.

2.2 Utlämnande på enskilds begäran

Det råder delade meningar om hur systemet för bevisutbyte ska uppfattas. Kommissionen är i sin konsekvensbedömning av uppfattningen att ett utbyte av bevis i systemet sker till den enskilde. Den uppfattningen grundar sig på att den enskilde hela tiden har kontroll över överföringen genom att beviset bland annat först överförs till den enskildes utrymme för förhandsgranskning. Detta synsätt kan enligt svensk rätt anses motsvara en begäran om utlämnande av allmän handling från den enskilde som sedan i sin tur delar beviset till den beviskonsumerande myndigheten. Ett sådant synsätt är juridiskt sett relativt okomplicerat och innebär inga särskilda juridiska problemställningar, se dock frågan om sekretess i avsnitt 3.

Ett annat synsätt är att se det tekniska systemet för bevisutbyte som ett utlämnande på enskilds begäran till en tredje part, det vill säga den beviskonsumerande myndigheten. Detta innebär att det är den enskilde som uppdragit att handlingen ska skickas till någon annan och ett sådant synsätt får ur ett rättsligt perspektiv anses motsvara att den enskilde själv begär ut beviset. Även detta synsätt kräver dock att det tekniska systemet innebär att den enskilde vidtar en åtgärd som kan anses motsvara en begäran från den enskilde.

2.3 Utlämnande mellan myndigheter

Regeringen uppdrog åt en sakkunnig att analysera och vid behov lämna förslag på hur SDG-förordningen ska kompletteras i nationell rätt. Uppdraget redovisades i en promemoria som bland annat kom fram till att det tekniska systemet för bevisutbyte är att anse som ett direkt utbyte mellan myndigheter, även om systemet bara ska användas på den enskildes uttryckliga begäran.[4] Denna slutsats grundades i att utbytet ska ske med tillämpning av engångsprincipen och att det skulle begränsas om systemet fick en utformning där utbytet går via den enskilde. Ett sådant synsätt kan innebära juridiska problemställningar om bevisen som överförs innehåller personuppgifter eller sekretessreglerade uppgifter. Om sekretess av sådant slag föreligger är det också osannolikt att en enskild kan efterge sekretessen för aktuella uppgifter.

[4] Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen) – En promemoria (I 2019:B), s. 113.

2.4 Förhandsgranskning

När ett bevis överförs från en behörig myndighet skickas det först till en processuell miljö där den enskilde ska kunna förhandsgranska beviset innan den enskilde väljer att överföra beviset till förfarandet. På det sätt den processuella miljön är uppbyggd och ska användas motsvarar det till viss del begreppet ”eget utrymme” som används i Sverige. Begreppet har etablerats under de senaste åren och blivit mer frekvent använt av myndigheter samt även bekräftats i förarbeten och praxis. Med eget utrymme menas enligt en definition av E-delegationen *ett skyddat förvar som tillhandahålls elektroniskt endast som led i teknisk bearbetning eller teknisk lagring för annans räkning*. Ett sådant utrymme föreligger bara när handlingar som förvaras där är undantagna från handlingsoffentlighet enligt 2 kap. 13 § första stycket TF. Enligt praxis är det väsentliga om myndighetens enda syfte med handlingarna är teknisk bearbetning eller lagring. Om myndigheten, av tekniska eller administrativa skäl, har möjlighet att använda handlingarna på något annat sätt är bestämmelsen inte tillämplig. Det egna utrymmet är ett utrymme som myndigheten tillhandahåller men som myndigheten samtidigt varken får ha insyn i eller har rätt att ta del av uppgifter i.

Den processuella miljön för förhandsgranskning i det tekniska systemet för bevisutbyte uppvisar vissa likheter med det svenska begreppet eget utrymme men det finns dock även vissa skillnader. Kommissionens senaste förslag på utkast till genomförandeakt innebär att ytan rent tekniskt kommer att vara placerad i den beviskonsumerade myndighetens land, det vill säga i det land där förfarandet inletts.[5] Detta innebär vissa juridiska problemställningar då beviset kommer att överföras till en annan medlemsstats tekniska yta. Uppgifterna i beviset är på så sätt redan expedierade och ”röjda” när de överförs till andra landets processuella miljö för förhandsgranskning.

En annan juridisk problemställning när det gäller den processuella miljön för förhandsgranskning är om den tekniska ytan ses på samma sätt i alla medlemsstater.

Ytterligare en juridisk problemställning är att det för närvarande inte står helt klart hur den tekniska ytan för förhandsgranskning kommer att vara uppbyggd och fungera och att det kan finnas en risk att den tekniska ytan inte kommer att

[5] Artikel 14 i kommissionens utkast till genomförandeakt.

uppfylla undantaget i 2 kap. 13 första stycket TF och att bevis som överförs till ytan i Sverige därmed kan utgöra allmänna handlingar. Juridiska problemställningar kopplade till GDPR utvecklas i avsnitt 5 om dataskydd. Sverige är av uppfattningen att den processuella miljön för att förhandsgranska ska ligga i det bevisproducerande landets tekniska yta. På det sättet undviker man problemställningen att beviset överförs till ett annat lands processuella miljö innan den enskilde valt att använda det aktuella beviset.

3 Sekretess

I bevisutbytet kommer bevis att utbytas som kan omfattas av sekretess enligt OSL. Enligt 3 kap. 1 § OSL innebär sekretess ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. I svensk rätt regleras sekretess oftast genom en verksamhetsspecifik bestämmelse eller en bestämmelse på generell nivå. I vanliga fall ska den myndighet som får en begäran om att lämna ut en handling göra en prövning om det förekommer någon sekretessbelagd uppgift och i så fall avgöra om någon sekretessbrytande bestämmelse är tillämplig. Utgångspunkten är alltså att myndigheten äger handlingen och är skyldig att pröva utlämnandet utifrån OSL.

För att uppfylla syftet med ett gränsöverskridande automatiskt bevisutbyte enligt engångsprincipen måste alla frågor om sekretess redan på förhand vara lösta. Det tekniska systemet är inte uppbyggt på ett sådant sätt att det kommer finnas en mekanism som i någon sekretessrättslig mening kommer att reagera på en begäran om överföring av ett bevis. Detta utgör en betydande juridisk problemställning och den är även nära sammankopplad med hur systemet ska uppfattas, det vill säga om det är ett utlämnande på enskilds begäran eller ett utbyte mellan myndigheter. Om det tekniska systemet ses som ett utlämnande till den enskilde uppkommer sällan frågan om sekretess då sekretess sällan gäller gentemot den enskilde. Om det tekniska systemet i stället ses som ett utbyte direkt mellan myndigheter kommer frågan om sekretess att aktualiseras. Så länge det inte finns en tydlig lagstiftning som medger undantag för sekretess eller en uppgiftsskyldighet för myndigheter att exportera uppgifter, kan det bli problematiskt att överföra uppgifter utifrån den föreslagna modellen. En tillkommande svårighet är även att det inte enbart är den enskilde som kommer att ta del av beviset utan det kan vara flera aktörer som inom ramen för det tekniska systemet kommer att ta del av beviset och ha rådighet över det, till exempel leverantörer av olika tekniska lösningar.

En annan juridisk problemställning som skulle kunna uppkomma, och som även är nära sammanbunden med dataskyddsfrågorna som aktualiseras (se avsnitt 5), är att sekretess kan gälla enligt 21 kap. 7 § OSL för uppgift om det kan antas att uppgiften kommer att behandlas i strid med 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 (dataskyddsförordningen) eller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Eftersom det finns en stor osäkerhet kring hur tillförlitligt dataskyddet kommer att vara gällande det tekniska systemet för bevisutbytet finns det en risk att det kan antas att personuppgifter kommer att behandlas i strid med bestämmelserna. Mot denna bakgrund finns en risk att denna bestämmelse kan komma att vara tillämplig.

3.1 Samtycke

Som angetts ovan innebär sekretess ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Det finns olika uppfattningar om när en uppgift är röjd, om det krävs att någon faktiskt har tagit del av uppgiften eller om det är tillräckligt att uppgiften gjorts tillgänglig.

Den enskilde kan häva sekretess som gäller gentemot sig själv helt eller delvis.[6] Det kan därför vara ett alternativ att se den enskildes användande av det tekniska systemet som att den enskilde samtycker till röjandet av uppgifterna. En tillkommande problemställning är dock att det kan finnas andra, t.ex. privata, aktörer eller leverantörer som bidrar med olika tekniska lösningar som uppgifterna då också kan anses röjda i förhållande till. Ett samtycke kan inte heller vara generellt utan kräver viss precision i förhållande till när och gentemot vem eller vilka det gäller. Det innebär därför vissa praktiska tillämpningssvårigheter när det gäller att använda en sådan sekretessbrytande grund i det tekniska systemet för automatiskt bevisutbyte. En annan problemställning kan uppstå om beviset innehåller uppgifter där det råder sekretess som träffar en tredje person eftersom även den personen i sådana fall måste lämna sitt samtycke.

[6] 10 kap. 1 § och 12 kap. 1-2 §§ OSL.

3.2 Sekretess enligt 8 kap. 3 § OSL

Om sekretess gäller för en uppgift finns begränsningar i OSL när det gäller utlämnande av sådana uppgifter till utländska myndigheter. Av 8 kap. 3 § OSL följer att en uppgift för vilken sekretess gäller inte får röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte 1) utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller 2) uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen. Bestämmelsen består alltså av två olika grunder för när sekretessreglerade uppgifter får röjas för en utländsk myndighet.

Om det tekniska systemet för bevisutbyte ses som ett utbyte mellan myndigheter utgör bestämmelsen därmed ett hinder mot ett automatiskt bevisutbyte. Det torde vara mest lämpligt att skapa förutsättningar för ett bevisutbyte genom kompletterande lagstiftning, det vill säga med stöd i bestämmelsens första punkt.[7] Att möta SDG-förordningens krav på ett automatiserat utbyte av bevis med en tvåstegsprövning enligt bestämmelsens andra punkt synes inte särskilt lämpligt eftersom den prövningen varken framstår som ändamålsenlig eller effektiv.[8]

4 Identitetsmatchning

SDG-förordningen ställer krav på att förfaranden ska kunna utföras helt online med innebörden att den enskilde användaren bland annat kan identifiera sig online.[9] För att uppfylla detta krav och för att det ska vara möjligt att koppla rätt bevis till den aktuella användaren krävs en identitetsmatchning. Det krävs att medlemsstaterna effektivt implementerar eIDAS-förordningen för att uppfylla SDG-förordningen.[10] Förfaranden i Sverige som ställer krav på svenskt personnummer eller samordningsnummer för tillgång till digitala tjänster eller

[7] Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen) – En promemoria (I 2019:B), s. 114.
[8] A.a., s. 114.
[9] Artikel 6 (2) (a) i SDG-förordningen.
[10] Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen) – En promemoria (I 2019:B), s. 98.

onlineförfaranden är en begränsning som kan vara oförenlig med ett uppfyllande av SDG-förordningens icke-diskriminerande krav.

En förutsättning för att genomföra en identitetsmatchning är att de personuppgifter som ingår i en utländsk e-legitimation kan jämföras mot personuppgifter som finns registrerade om den enskilde hos en behörig myndighet i Sverige och i svenska folkbokföringen. Uppgifter som får behandlas i folkbokföringen regleras dels i en lag (2001:182), dels en förordning (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Av 2 kap. 10 § första stycket lag om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet framgår att vissa uppgifter, till exempel födelseort, inte får användas som sökbegrepp vid sökning och urval i folkbokföringen. Inom eIDAS är födelseort ett valfritt attribut. Uppgift om medborgskarskap får användas som sökbegrepp endast i fråga om medborgarskap i Sverige, Danmark, Norge, Finland eller Island samt om medborgarskap inom eller utom Europeiska unionen (unionsmedborgarskap eller icke unionsmedborgarskap). Det är därmed förbjudet att söka på uppgift om medborgarskap i t.ex. Tyskland, Frankrike, Spanien eller Italien.

I bestämmelsen om för vilka ändamål personuppgiftsbehandling i folkbokföringen får ske saknas matchning av identiteter eller något motsvarande.[11] Däremot finns en punkt om *uttag av urval av personuppgifter* som relaterar till sökning. Det bör därför undersökas inom ramen för en fortsatt juridisk analys om matchning av uppgifter kan jämställas med sökning och urval eller om det behövs kompletteringar av bestämmelsen om för vilka ändamål personuppgiftsbehandling får ske.

Av bestämmelsen om direktåtkomst till folkbokföringen framgår att en myndighet får ha direktåtkomst till uppgift om person- eller samordningsnummer, namn, adress, folkbokföringsfastighet, lägenhetsnummer, distrikt och folkbokföringsort samt avregistrering från folkbokföringen.[12] En myndighet får även ha direktåtkomst till andra uppgifter i folkbokföringen om myndigheten behöver uppgifterna för att fullgöra sitt uppdrag och får behandla dem (med undantag för

[11] Se 1 kap. 4 § första stycket lag om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet.
[12] Se 2 kap. 8 § första stycket lag om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet.

om det är olämpligt ur integritetssynpunkt).[13] Det behövs en fortsatt analys kring om det är ändamålsenligt att behöriga myndigheter får möjlighet att själva nyttja folkbokföringen för identitetsmatchning eller om det ska centraliseras till en enskild myndighet, till exempel Skatteverket. I samband med detta bör det även analyseras vilka författningsändringar som är nödvändiga för att behöriga myndigheter som inte är förvaltningsmyndigheter (t.ex. Sveriges a-kassor) ska få likvärdiga möjligheter till identitetsmatchning som förvaltningsmyndigheterna.

En ytterligare problemställning är det krav på identitetsmatchning som föreslagits i artikel 16 i utkastet till genomförandeakt för det tekniska systemet för bevisutbyte. I artikeln klargörs att bevis från behöriga myndigheter endast ska lämnas ut om processen för identitetsmatchning resulterar i en s.k. ”otvetydig matchning”. Det är oklart vad som avses med det begreppet i juridisk mening. Juridiska problemställningar med identitetsmatchning kan uppstå avseende till exempel hur personer som har bytt personnummer eller namn ska hanteras (beviset finns registrerat i tidigare identitet men inloggning sker med nuvarande identitet).

5 Dataskyddsregleringen

Av artikel 2 i dataskyddsförordningen framgår att förordningen är tillämplig på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Det står klart att personuppgifter kommer att behandlas på ett vis som medför att dataskyddsförordningen ska tillämpas när bevis utbyts i systemet. Det är viktigt att det tekniska systemet för bevisutbyte uppfyller dataskyddsförordningens bestämmelser, vilket även anges i SDG-förordningen.[14] Det finns flera risker, snarare än juridiska problemställningar, kopplade till det tekniska systemet för bevisutbyte vilket vi kommer att behandla i de följande avsnitten.

[13] Se 2 kap. 8 § andra stycket lag om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet.
[14] Artikel 33 SDG-förordningen.

5.1 Personuppgiftsansvarig

En personuppgiftsansvarig är enligt dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.[15]

Det är de faktiska omständigheterna i det enskilda fallet som är avgörande för bedömningen av vem som är personuppgiftsansvarig, dvs. vem eller vilka som har bestämt över behandlingen. Avgörande för denna bedömning är bland annat, varför behandlingen utförs och vem som är initiativtagare till behandlingen. Det bör analyseras hur personuppgiftsansvaret ska fördelas vid respektive behandling av personuppgifter inom ramen för det tekniska systemet.

5.1.1 Ansvaret vid överföring till utrymmet för förhandsgranskning

En risk när det gäller personuppgiftsbehandlingen i det tekniska systemet för bevisutbyte rör överföringen av beviset till den tekniska ytan för förhandsgranskning. Enligt kommissionens senaste förslag ska den processuella miljön förläggas i den mottagande medlemsstaten, det vill säga den beviskonsumerande medlemsstaten.[16] Mycket talar därför för att, utifrån svensk rätt, att den medlemsstat där ytan tekniskt sett är placerad kommer att tillhandahålla ytan och därför sannolikt blir personuppgiftsansvarig för behandlingen som sker i ytan för förhandsgranskning.[17] Problemen består då bland annat i att mottagande myndighet kommer få svårt att beakta principerna om uppgiftsminimering samt säkerställa rättslig grund för behandling av personuppgifter som inte efterfrågats av användaren men ändå överförts eftersom de utgör en del av beviset. Därutöver kan problem uppstå till följd av det svenska regelverket om bevarande av allmänna handlingar. Det går att argumentera för att en svensk myndighet blir skyldiga att arkivera uppgifter som mottagits inom

[15] Artikel 4.7 dataskyddsförordningen.
[16] Artikel 14 i kommissionens senaste utkast till genomförandeakt.
[17] Förvaltningsrätten i Stockholms dom meddelad den 24 maj 2018 i mål nr 11458-17.

ramen för bevisutbytet, förutsatt att uppgifterna kommer från utomstående myndighet, så snart de når den svenska myndighetens egna utrymme. En fördel med att den processuella miljön placeras i det bevisproducerande landet är att beviset då inte behöver överföras till ett annat land innan användaren väljer vilket bevis som denne ska ge in. Det blir även då tydligare vem som är personuppgiftsansvarig.

5.2 Principer för behandling av personuppgifter

Enligt dataskyddsförordningen måste varje behandling av personuppgifter uppfylla vissa principer. När det gäller bevisutbytet ser vi risker främst i förhållande till principen om uppgiftsminimering. De behandlade personuppgifterna ska enligt principen vara adekvata och relevanta i förhållande till ändamålen för behandlingen. Det innebär att ovidkommande personuppgifter inte får behandlas.

De behandlade personuppgifterna får inte heller vara för omfattande i förhållande till ändamålen för behandlingen. Det är alltså inte tillåtet att behandla fler personuppgifter än som är nödvändigt för att kunna uppfylla ändamålen för behandlingen. Inom systemet kan det bli aktuellt att utbyta bevis för ett förfarande där beviset innehåller fler uppgifter än vad som behövs i förfarandet, vilket kan vara i strid med principen om uppgiftsminimering.

5.3 Grund för behandling

För att få behandla personuppgifter krävs enligt dataskyddsförordningen en rättslig grund för behandlingen. Detta innebär att någon av grunderna i artikel 6 i dataskyddsförordningen måste vara uppfylld vid varje form av behandling. Enligt kommissionen måste man skilja på rättslig grund för behöriga myndigheter när det gäller i) att begära bevis för ett visst förfarande, ii) att tillhandahålla ett bevis, och iii) att använda det tekniska systemet.

För i) och ii) föreskrivs den rättsliga grunden enligt kommissionen i nationell rätt eller unionslagstiftningen. Det gäller till exempel vilka bevis som kan krävas av en användare för vissa förfaranden, i vilka situationer och på vilken grund bevisen innehas av en behörig myndighet för att överlämnas till en annan behörig myndighet eller tillhandahållas en användare. Skäl 45 i SDG-förordningen påminner om att gränsöverskridande utbyte av bevis bör ha en tillämplig rättslig grund såsom direktiv 2005/36/EU (erkännande av yrkeskvalifikationer),

2006/123/ EU (tjänster på den inre marknaden), 2014/24/EU (offentlig upphandling) eller 2014/25/EU (upphandling inom vatten, energi, transporter, posttjänster) eller, för de förfaranden som anges i bilaga II till SDG-förordningen, annan tillämplig unionslagstiftning eller nationell lagstiftning. Kommissionen anser också att en begäran från användare inte kan likställas med samtycke enligt artikel 6 (1) (a) GDPR. Samtycke är inte heller en lämplig rättslig grund för myndigheter att använda sig av.[18] När det gäller rättslig förpliktelse är det inte heller tillräckligt då regleringen i SDG-förordningen om bevisutbytet inte torde vara en tillräckligt preciserad och detaljerad förpliktelse.[19] Det finns behov av att närmare fastställa rättslig grund för samtliga behandlingar inom ramen för det tekniska systemet för bevisutbyte.

6 Myndighetsspecifika juridiska problemställningar

Vissa juridiska problemställningar är inte av sådan karaktär att de flesta behöriga myndigheterna berörs av problemställningarna, det vill säga det är problemställningar av mer myndighetsspecifik karaktär. En sådan problemställning som har identifierats av flera myndigheter är registerförfattningar som kan utgöra ett hinder mot att lämna ut bevis elektroniskt.

Centrala Studiestödsnämnden (CSN) har angett att deras registerförfattningar studiestödsdatalagen (2009:287), som innehåller bestämmelser om lagens tillämpningsområde, tillåtna ändamål för behandling av personuppgifter och de begränsningar som ska gälla för användningen av uppgifterna samt studiestödsdataförordningen (2009:321) behöver ändras för att CSN ska kunna uppfylla kraven enligt bevisutbytet för överföring av bevis till utländsk myndighet enligt engångsprincipen. Med CSN:s gällande registerförfattning är ett sådant elektroniskt uppgiftsutlämnande inte tillåtet. Även Skatteverket har identifierat att

[18] Skäl 43 till dataskyddsförordningen.

[19] Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen) – En promemoria (I 2019:B), s. 89.

registerlagstiftning kan utgöra ett hinder mot ett elektroniskt bevisutbyte enligt engångsprincipen.

Transportstyrelsen har angett att myndigheten styrs av olika registerlagar för olika bevis. Ett exempel som myndigheten har lyft fram är lokförarbevis. Transportstyrelsen för ett register över lokförarbevis och uppgifter om beviset hämtas därifrån. När det gäller den regleringen finns vissa begränsningar vad gäller elektroniskt utlämnande. Om systemet för bevisutbyte enligt engångsprincipen ses som att uppgifterna lämnas till den begärande myndighet så är det begränsat till vem eller vilka som uppgifter får lämnas elektroniskt (bevis får lämnas elektronisk till den som är registrerad i förarbevisregistret när det gäller uppgifter om den registrerade själv, olycksutredande myndighet i Sverige, behörig järnvägssäkerhetsmyndighet och behörigt olycksutredande organ i annat land inom EES eller i Schweiz, Europeiska järnvägsbyrån, och det järnvägsföretag eller den infrastrukturförvaltare i vars verksamhet föraren är anställd eller anlitad). Det föreligger dock ingen begränsning i förhållande till den enskilde.

En ytterligare problemställning som flera myndigheter har beskrivit är att det är svårt för myndigheterna att tolka SDG-förordningens tillämpningsområde när det gäller det tekniska systemet för bevisutbyte. Det innebär att många myndigheter riskerar att göra felbedömningar i huruvida myndigheten omfattas av det tekniska systemet för bevisutbyte och flera myndigheter efterfrågar mer stöd i den frågan.