



Rättslig analys

Bilaga till rapporten Delrapportering av uppdrag att tillhandhålla infrastruktur för säker digital kommunikation i offentlig sektor (dnr 2021-2909)

Innehållsförteckning

1	Inledning	3
2	Dataskydd och sekretess	4
2.1	Slutsats och/eller rekommendation	4
2.2	Inledning	4
2.3	Informationsflödet utifrån ett sekretesshänseende	5
2.3.1	Teknisk bearbetning eller teknisk lagring	5
2.3.2	Bedömning	7
2.4	Informationsflödet utifrån ett dataskyddsperspektiv	10
2.5	Adressboken	11
2.5.1	Adressbokens funktionalitet i förhållande till sekretess	13
2.5.2	Adressbokens funktionalitet i förhållande till dataskyddsförordningen	14
2.6	Val av leverantörer	16
2.6.1	Sekretessfråga vid val av leverantörer	16
2.6.2	Dataskyddsfrågor vid val av leverantörer	17
2.6.3	SDK:s kryptering i förhållande till tredjelandsoverföringar	17
3	Privata aktörer och konkurrens	19
3.1	Slutsats och/eller rekommendation	19
3.2	Inledning	19
3.3	KOS-reglerna	20
3.3.2	Praxis	22
3.4	Bedömning	24
3.4.1	Är SDK en ekonomisk verksamhet som utgör ett företag	24
3.4.2	Är förfarandet försvarbart från allmän synpunkt	26
3.4.3	Är det säljverksamheten eller ett specifikt förfarande som ev. är konkurrensbegränsande	28
3.4.4	Resulterar säljverksamheten eller förfarandet en snedvridning eller hämmande av konkurrensen	28
4	Upphandling	29
4.1	Slutsats och/eller rekommendation	29
4.2	Inledning	29
4.3	Tillämpliga bestämmelser, m.m.	30
4.3.1	Upphandlingspliktiga anskaffningar, särskilt om kontraktsbegreppet och tilldelning av kontrakt	30

4.3.2	Potentiellt tillämpliga undantag.....	34
4.4	<i>Bedömning</i>	40
4.4.1	Deltagarnas tillträde till och användning av SDK.....	41
4.4.2	Anskaffning av eventuella tredjepartstjänster	42
4.4.3	Ev. underleverantörers roller	44
4.4.4	Tillhandahållandet av SDK i samverkan med en offentligrättslig samarbetspartner – Hamburgundantaget	47

1 Inledning

Denna bilaga är en del av rapporten *Delrapportering av uppdrag att tillhandahålla infrastruktur för säker digital kommunikation i offentlig sektor*. I rapporten har DIGG redovisat de rättsliga övervägande på en övergripande nivå. I denna bilaga analysera de rättsliga frågorna som aktualiseras i och med Säker digital kommunikation (SDK) mer utförligt. De frågor som DIGG har identifierat som relevanta är frågor om dataskydd och sekretess, konkurrensbegränsande offentlig säljverksamhet, upphandling samt avtalsmodell och ansvarsfördelning. Delen om avtalsmodell och ansvarsfördelning finns endast i rapporten eftersom den inte är så omfattande.

I det följande redogörs översiktligt för den planerade infrastrukturen SDK. Beskrivningarna är mycket förenklade och syftar i första hand till att utgöra en bakgrund till den rättsliga analysen.

SDK bygger i grunden på en plattform. Plattformen definierar gemensamma regler för samverkan och ägs och förvaltas av en plattformsansvarig. Den som är plattformsansvarig ansvarar bland annat för ramverk och specifikationer.

Till plattformen är SDK-federationen ansluten. För en federation ansvarar en federationsägare, vilken är en juridisk person som äger och förvaltar federationen inom ramen för plattformen. Inom ramen för federationen tillhandahåller federationsägaren (i förekommande fall med hjälp av underleverantörer) olika typer av federationstjänster till deltagarna, exempelvis en adressbok och testbäddstjänster. Vidare tillhandahålls plattformstjänster, såsom SML, SMP, CertPub, PKI och testbäddstjänster av plattformsansvarig. Även externa tjänster och särskilda deltagartjänster kan komma att tillhandahållas till deltagarna inom ramen för federationen, exempelvis identitets- och meddelandetjänster.

Deltagare i SDK kan vara offentliga aktörer, statliga myndigheter, regioner och kommuner, offentligt ägda bolag med flera samt privata aktörer. Vilka privata aktörer som kommer att kunna ansluta och i vilken omfattning beror på behovet hos offentlig sektor.

Godkända tredjepartsleverantörer tillhandahåller tjänster inom ramen för SDK. En sådan typ av leverantör är accesspunktsoperatören som tillhandahåller accesspunktslösningar för deltagare, det vill säga lösningar för anslutning och

kommunikation i SDK. En deltagare kan även själv ikläda sig rollen som accesspunktsoperatör, om kapacitet för detta finns internt.

2 Dataskydd och sekretess

2.1 Slutsats och/eller rekommendation

Det är viktigt att noga analysera frågorna om dataskydd och sekretess med hänsyn till att SDK har som syfte att hantera stora mängder känslig och sekretessbelagd information, inbegripet personuppgifter. För att säkerställa en godtagbar säkerhet för personuppgifter och sekretessbelagd information är det viktigt att utformningen av SDK anpassas utifrån organisatoriska och tekniska säkerhetsåtgärder som möter de krav som ställs på sådan information. Detta ställer bland annat krav på utformningen av ingående komponenter samt vilka som kan vara leverantör av dessa komponenter.

2.2 Inledning

I denna del analyseras dataskydds- och sekretessfrågor som uppstår i informationsflödet inom SDK.

Med informationsflödet avses kedjan från det att information skickas från en avsändare till att informationen når mottagaren, inbegripet hanteringen som sker hos accesspunkterna, meddelandetjänsten och meddelandeklienten. Däremot avses inte enskilda deltagares informationsflöden som uppstår inför att information ska skickas eller efter det att information tagits emot. Frågor om rättsliga grunder utifrån Europaparlamentets och rådets förordning (EU) 2016/679 (dataskyddsförordningen) för den deltagande myndighetens egen behandling vid anslutning till SDK och i samband med att information skickas eller tas emot inom infrastrukturen berörs inte heller i detta avsnitt. Detsamma gäller bedömningar om det finns sekretessbrytande bestämmelser om att röja uppgifter till en slutmottagare enligt offentlighets- och sekretesslagen (2009:400), (OSL). Sådana frågor ankommer på deltagande myndigheter själva att avgöra inför varje enskilt utlämnande.

2.3 Informationsflödet utifrån ett sekretesshänseende

2.3.1 Teknisk bearbetning eller teknisk lagring

Accesspunktoperatörernas hantering av krypterad information inom SDK omfattas av definition av teknisk bearbetning eller teknisk lagring i tryckhetsförordningen.

2.3.1.1 *Relevanta bestämmelser, m.m.*

Av 2 kap. 9 § 3 st. och 2 kap. 13 § 1 st. tryckfrihetsförordningen (TF) framgår att en åtgärd som någon vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit inte ska anses leda till att handlingen har kommit in till den myndigheten och en handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses inte som allmän handling hos den myndigheten.

Genom 4§ lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller teknisk lagring av uppgifter (tystnadspliktslagen) åläggs anställda hos tjänsteleverantörer en tystnadsplikt för de uppgifter de får del av när en myndighet anlitar dem för att tekniskt bearbeta eller tekniskt lagra information. Av förarbetena till tystnadspliktslagen framgår att innebörden av teknisk bearbetning och teknisk lagring är densamma som i TF.¹

Teknisk bearbetning eller teknisk lagring definierades i förarbetena ursprungligen som överföring av maskinskrivet manuskript till magnetband, tryckning eller kopiering av manuskript, redigering av ljudupptagningar på magnetband, överföring av sådana uppgifter till grammofonskiva samt framkallning av

¹ Prop. 2019/20:201, s. 22.

fotografiskt material.² Det är dock inte helt klarlagt vad som anses utgöra teknisk bearbetning eller teknisk lagring.³

I praxis har frågan om vad som avses med teknisk bearbetning eller teknisk lagring definierats indirekt genom att pröva om en handling anses offentlig och därmed kan bli föremål för utlämnande i enlighet med offentlighetsprincipen. Handlingar som endast behandlas inom ramen för teknisk bearbetning eller teknisk lagring kan inte bli föremål för utlämnande. Rättstillämpningen är emellertid spretig beträffande vad som anses omfattas av teknisk bearbetning eller teknisk lagring. En förutsättning för bedömningen av definitionen är rekvisitetet ”*för annans räkning*”. Att någon endast lagrar uppgifter för annans räkning har i praxis definierats som teknisk bearbetning eller teknisk lagring, det vill säga den situationen att en myndighet anlitar annan aktör för att hantera information uteslutande för myndighetens räkning.⁴ Att tekniskt begränsa mottagande aktörens åtkomst har i praxis haft betydelse för definitionsbedömningen, till exempel där egna ändamål hos den aktör som drifvar för annans räkning (såsom ärendehantering och avsaknad av teknisk åtkomstbegränsning) talar för att handlingar inte endast hanteras för annans räkning och därigenom inte omfattas av definitionen teknisk bearbetning eller teknisk lagring.⁵ Det är däremot oklart vilken påverkan på bedömningen viss handpåläggning hos mottagande aktören har, det vill säga att mottagande aktör hanterar informationen dels för utlämnande myndighets räkning, dels för egen räkning och för egna ändamål.⁶

² Prop. 1975/76:160, s. 137 f.

³ Se bland annat prop. 2019/20:201 s. 13 ff. där flera remissinstanser önskat ett förtydligande av begreppet men där lagstiftaren i och för sig påtalade att det i praktiken inte torde medföra några tillämpningssvårigheter av begreppet annat än i ljuset av dagens, och framtidens, teknikanvändning och teknikutveckling. Precis vad som anförts i SOU 2021:97 s. 246 ff. har definitionen av teknisk bearbetning eller teknisk lagring inte alls varit självklar historiskt och till följd av detta varit föremål för domstolsprövningar vid ett flertal situationer. Detsamma framgår hos flera remissinstanser i remissyttrande till IT-driftsutredningen, delbetänkande SOU 2021:1, se bland annat Försäkringskassan FK2021/001872, s. 6.

⁴ RÅ 1994 ref. 64 och kammarrätten i Jönköping, mål nr 2692-10.

⁵ Kammarrätten i Jönköping, mål nr 3610-19 och HFD 2018 ref. 48.

⁶ HFD 2011 ref. 52, där bl.a. statistiska ändamål hos mottagande myndighet synes påverkat bedömningen att uppgifterna inte var föremål för teknisk bearbetning eller teknisk lagring. Jämför avgörandet i Kammarrätten i Stockholm, mål nr 1195-11, där utfallet blev annat för liknande omständigheter.

2.3.2 Bedömning

För att underlätta offentliga aktörers tolkning av sekretessen vid teknisk bearbetning eller teknisk lagring föreslår DIGG att det införs en sekretessbrytande bestämmelse för teknisk bearbetning eller teknisk lagring

2.3.2.1 *Är accesspunktsoperatörens hantering teknisk bearbetning eller teknisk lagring*

Frågan är om accesspunktsoperatör hantering av information inom SDK kan anses motsvara den tilltänkta tillämpningen för teknisk bearbetning eller teknisk lagring. Inom SDK ska all information som skickas från avsändare till mottagare vara krypterad för såväl utomstående som för accesspunktsoperatörerna. Inom accesspunkterna tillämpas ytterligare en kryptering innan informationen överförs till den mottagande deltagaren. I vissa fall driftas accesspunkterna hos deltagarna själva och i andra fall driftas accesspunkterna hos extern myndighet eller kommersiell leverantör. Bedömningen av vad som anses omfattas av definitionen teknisk bearbetning eller teknisk lagring är därför viktig för att avgöra vilket manöverutrymme myndigheterna har beträffande upprättande av accesspunkter och eventuell utkontraktering av accesspunktleverantörer.

Vid en sammantagen bedömning går det i vart fall argumentera för att förhållanden där en part uteslutande hanterar data för annans räkning och inte har egna ändamål samt att åtkomst begränsas tekniskt för mottagande aktör (i det här fallet accesspunkterna) endast sker för teknisk bearbetning eller teknisk lagring. Anförandet är även i linje med det resonemang som fördes till begreppsdefinitionen vid införandet av tystnadspliktslagen.⁷

I och med att upplägget i SDK baseras på att data överförs krypterad till accesspunktsoperatörer, som både saknar teknisk åtkomst till uppgifterna och endast behandlar uppgifterna på utlämnande myndighets instruktioner, är bedömningen att åtgärderna som vidtas hos accesspunktsoperatören endast utgör ett led i en teknisk bearbetning eller teknisk lagring.

⁷ Prop. 2019/20:201, s. 22 f.

2.3.2.2 Rövande av uppgifter till accesspunktsoperatörerna

Frågan om när och i vilken omfattning uppgifter röjs vid teknisk bearbetning eller teknisk lagring har under en längre tid varit en omdiskuterad fråga. En utbredd ståndpunkt har sedan tidigare varit att sekretessuppgifter som endast är föremål för teknisk bearbetning eller teknisk lagring inte röjs till den utomstående som vidtar åtgärder för detta ändamål. I huvudsak kan resonemanget härledas till utgångspunkten att uppgifter som endast varit föremål för teknisk bearbetning eller teknisk lagring inte definierats som vare sig inkommen eller expedierad och således aldrig lämnat en myndighets sekretessfär.⁸ Därtill har rättsutvecklingen förtydligat att det i den civilrättsliga ordningen går att organisera ett förhållande så att ett subjekt som annars inte skulle omfattats av straffsanktionerad tystnadsplikt, ändå gör det.⁹

Praxis är oklar beträffande rövandebegreppet. Samma rättskällor har åberopats i decennier av olika aktörer med ibland helt olika bedömningar och slutsatser. Särskilt fokus har varit NJA 1991 s. 103 (frågan om innebörden av uttrycket "röjt uppgift" i 19 kap. 9 § BrB om straffbarhet till följd av vårdslöshet med hemlig uppgift) och JO 1982/73 s. 238 (om utkontraktering till servicebyråer) i förhållande till JO 2014-09-09, dnr 3032-2011, (om utkontraktering av läkarsekreterare).

Ett prejudikat som inte bör tillmätas någon större betydelse i förhållande till utkontraktering kopplat till rövandebegreppet för SDK är NJA 1991 s. 103. Visserligen fördes resonemang om vårdslöshet med hemlig uppgift och vissa resonemang om sannolikhet och besittning. Det går dock inte bortse från att domstolen prövade den straffrättsliga frågan mot enskild i förhållande till den straffsanktionerade tystnadsplikten. Det är svårt att utröna om bedömningen varit densamma om rövande frågan prövats gentemot en myndighet och att myndigheten beslutat om att förvara sekretesskyddade handlingar i skåp som inte uppfyllt adekvata säkerhetskrav.

I ett försök att finna en enhetlig rättstillämpning tolkar DIGG JO:s beslut om läkarsekreterare som att JO främst uppmärksammade det faktum att civilrättsliga avtal, som inte kan likställas en straffsanktionerad tystnadsplikt, inte alltid kan

⁸ Prop. 1975/76:160, s. 137 f.

⁹ Prop. 1979/80:2, del A, s. 128 f, Lagkommentar till 2 kap. 1 § OSL från JUNO (Lexino) där bl.a. ett resonemang om förbehåll utifrån 10 kap.14 § OSL finns), , lagkommentar 2 kap. 1 § OSL från JUNO (Norstedts juridik), JO 1982/83 s. 238.

medföra att utkontraktering anses förenlig med sekretessbestämmelserna och att omständigheterna kan medföra att en sekretessbrytande bestämmelse behövs vid utkontraktering. Detta till skillnad från JO:s beslut om servicebyråer där omständigheterna och därtill det civilrättsliga avtalet beträffandet upplägget mellan parterna medförde att sekretessuppgifterna aldrig var att anse som röjda. JO tar inte ställning i något av besluten till frågan om utlämnande för teknisk bearbetning eller teknisk lagring medför att sekretessuppgifter röjs.

I IT-driftsutredningen fördes ett resonemang om att utkontraktering alltid medför att uppgifterna som är föremål för utkontrakteringen röjs, oavsett om utkontraktering skett inom ramen för teknisk bearbetning eller teknisk lagring och oavsett om uppgifterna är krypterade även för mottagande deltagare.¹⁰ DIGG anser att det finns en logik i IT-driftsutredningens strikta bedömning av röjandebegreppet. Det går att ifrågasätta behovet av tystnadspliktsbestämmelser i 11 kap. 4 § a OSL om uppgifter aldrig ansetts lämnat sekretessfären och således blivit röjda (även om resonemanget går emot en hos vissa sedan tidigare inarbetad etablerad praxis beträffande röjandebegreppet). IT-driftsutredningens förslag har mött ett stort motstånd av remissinstanserna, inte minst beträffande ställningstagandet om att även krypterade uppgifter alltid ska anses som röjda.¹¹ Något som kan haft betydelse för meningsskiljaktigheterna är myndigheternas olika tolkningar av begreppet teknisk bearbetning eller teknisk lagring.¹² Vissa myndigheter förespråkar en vidare tolkning av begreppet som innebär att den som tar emot information för teknisk bearbetning eller teknisk lagring även har visst utrymme att behandla informationen för egna syften, såsom statistikändamål. Denna tolkning av begreppet medför att det är avsevärt svårare att argumentera för att uppgifter inte röjs för annan aktör eftersom den mottagande aktören hanterar information för egna syften och får ta del av okrypterad informationen. Dessutom aktualiseras frågorna om sekretessbrytande bestämmelser och sekretessavtalens juridiska tillkortakommanden. Andra myndigheter tillämpar en snävare tolkning av begreppet som innebär att den som tar emot informationen

¹⁰ SOU 2021:1, s. 281–283.

¹¹ Se bland annat följande remissvar: Arbetsförmedlingen (Af-2021/0008 2776, s.4 ff.), E-Hälsomyndigheten (2021/00541 s.1 f.), Försvarsmakten (FM2021-4977:3, s. 1), Försäkringskassan (FK2021/001872 s.3 f.), Myndighet för digital förvaltning (2021-185 s. 2 och 4).

¹² Vilket påtalades i flera remissvar enligt ovan men även i Skatteverkets remissvar (8-744868, s. 3 f.). Detta lyftes även av remissinstanserna inför prop. 2019/20:201 men som lagstiftaren aktivt valt att inte besvara och där otydlighet beträffande definitionen tydliggjordes i SOU 2021:97.

endast får hantera informationen i krypterad form och på den avsändande myndighetens instruktioner. Denna tolkning av begreppet medför att det är lättare att argumentera för att uppgifterna inte röjs.

För nu aktuell situation med SDK krypteras uppgifterna från avsändaren till mottagaren. Krypteringen hålls intakt även gentemot accesspunktsoperatören. För att en accesspunktsoperatör ska få åtkomst till uppgifterna måste accesspunktsoperatören agera mot myndigheternas instruktioner och med hjälp av brottsliga medel dekryptera uppgifterna.

I enlighet med DIGGs remissvar till IT-driftsutredningen är bedömningen att uppgifterna i SDK hanteras och organiseras civilrättsligt på ett sådant sätt att uppgifterna inte är att betrakta som röjda till accesspunktsoperatörerna.

För att klargöra möjligheterna att byta information inom SDK, och därmed underlätta för samtliga offentliga deltagare att nyttja SDK oavsett tolkning av begreppen teknisk bearbetning eller teknisk lagring samt röjande, föreslår DIGG att en sekretessbrytande bestämmelse införs avseende teknisk bearbetning eller teknisk lagring i enlighet med IT-driftsutredningens förslag.

2.4 Informationsflödet utifrån ett dataskyddsperspektiv

Varje deltagare är självständigt personuppgiftsansvarig för den information som skickas inom SDK.

Personuppgiftsbiträdesförhållande kan dock uppstå vid utkontraktering av accesspunkttertjänster, meddelandetjänster och meddelandeklienter.

Inom ramen för DIGGs ansvar för SDK är DIGG självständigt personuppgiftsansvarig.

En utgångspunkt inom nuvarande SDK-infrastruktur hos Inera är att deltagarna själva är personuppgiftsansvarig för informationsflödet. Personuppgiftsansvaret för den avsändande deltagaren innebär att denne har ansvar att bedöma lagligheten och lämpligheten av att skicka personuppgifterna medan den mottagande deltagaren har ansvar för samma personuppgifter när denne tar emot dessa via sin accesspunkt. Samma bedömning görs för SDK som DIGG ska tillhandahålla.

Beroende på vad anslutande deltagare väljer att utkontraktera kan ett personuppgiftsbiträdesförhållande uppstå gentemot leverantörer av accesspunkter, meddelandetjänster och meddelandeklienter.

Inom ramen för DIGGs ansvar för SDK behöver DIGG samla in uppgifter från anslutande deltagare med ändamålet att administrera komponenterna i SDK, såsom adressboken. För dessa uppgifter är DIGG personuppgiftsansvarig.

Det är viktigt att respektive anslutande deltagare säkerställer en adekvat nivå av teknisk och organisatorisk säkerhet i samband med att nödvändiga tjänster och komponenter för att kunna delta i SDK utkontrakteras, inbegripet genomförande av rättsliga analyser, upprättande av konsekvensbedömningar och personuppgiftsbiträdesavtal.

2.5 Adressboken

Det är viktigt att samtliga aktörer säkerställer en detaljerad och korrekt nivå av funktionsadresser av sina organisationer i adressboken för att undvika att information röjs. I händelse av att adressboken innehåller funktionsadresser som inte är på rätt verksamhetsnivå eller är felaktiga riskerar uppgifter röjas till obehöriga verksamhetsgrenar inom samma organisation, vilket kan orsaka problem gällande sekretess och personuppgiftsbehandlingar.

DIGG avser att analysera vilka åtgärder som behöver vidtas för att säkerställa en korrekt hantering av funktionsadresserna i adressboken.

Frågan som avses hanteras i detta avsnitt tar sikte på rättsliga problem som kan uppstå till följd av adressbokens struktur och tillämpning. Frågorna att ta ställning till är vilket ansvar en mottagande deltagare har för den information som denne får ta emot inom SDK när det gäller personuppgiftsansvar och ansvar för sekretessbelagd information. Utgångspunkten är att majoriteten av de anslutande deltagarna kommer att omfattas av skyldigheten att följa OSL och dataskyddsförordningen samt anknytande lagstiftning. Avsnittet avser inte hantera frågan om betydelsen av huruvida en myndighet har en sekretessbrytande bestämmelse för viss informationsmängd till en specifik mottagare. DIGG förutsätter att anslutande myndigheter löpande kommer sekretesspröva sina utlämnanden.

SKR har i en tidigare rapport från år 2016 problematiserat bland annat frågan om att säkerställa rätt mottagare vid utlämnande av digitala meddelanden och konstaterade att det då inte fanns något enhetligt mottaganderegister för digitala meddelanden.¹³ Inera har därefter antagit uppdraget att upprätta en adressbok för anslutande deltagare. Förfarandet med adressboken för SDK hos Inera innebär att deltagarna själva underhåller och ansvarar för sina funktionsadresser medan Inera lägger upp och tilldelar administratörsrättigheter till anslutna deltagare.¹⁴

De juridiska frågorna kring förfarandet med adressboken har berörts inom ramen för regeringsuppdraget (I2020/02241/DF) *Kommuner och regioners förutsättningar att ansluta och delta i den förvaltningsgemensamma digitala SDK, Fallstudie: Säker digital kommunikation, SDK* och i Ineras egna rapport *Säker digital kommunikation 2021–2022 – Gemensam pilotrapport, version 1.0 (2022)*. Sammanfattningsvis har frågor lyfts beträffande hur avsändande deltagare ska kunna säkerställa att de skickar information till rätt mottagare.

I nuvarande SDK-infrastruktur hos Inera finns kodverk upprättade som stödjer strukturerad sökning av funktionsadresser och underlättar för deltagare att hitta rätt mottagare i en organisation. En funktionsadress kan tilldelas en eller flera koder i ett kodverk för att möjliggöra exakta sökningar. Genom att tilldela en funktionsadress koder från ett av adressbokens kodverk möjliggörs för andra deltagare att söka fram funktionsadressen genom filtrering utifrån koder i kodverket. Den som söker behöver således inte känna till det exakta namnet på funktionsadressen som sökes, utan kan söka fram funktionen utifrån exempelvis ett verksamhetsområde via en kod i ett kodverk.¹⁵

En korrekt behörighetshantering hos den administrativa funktionen som har åtkomst till krypteringsnycklarna torde inte medföra några omfattande juridiska problem. Nuvarande upplägg förutsätter dock en tillfredställande informationssäkerhet hos deltagare inom SDK. Omvänt kan en bristfällig informationssäkerhet där krypteringsnycklarna hanteras på ett icke godtagbart sätt sett till säkerheten medföra att sekretessuppgifter riskeras röjas. För en sådan

¹³ SKL Slutrapport, version 1.1, 2016-03-31, *Säker digital meddelandehantering – Nuläges- behovs- och marknadsanalys*.

¹⁴ Inera, version 1.0.3, 2020-12-10, *End-to-end-säkerhet – förutsättningar och krav*.

¹⁵ Inera, version 1.2, 2022-06-17. *Säker digital kommunikation – användarhandledning för administratörer i SDK Adressbok*.

situation aktualiseras även frågan om en tillräcklig teknisk- och organisatorisk säkerhetsnivå i förhållande till kraven i dataskyddsförordningen.

2.5.1 Adressbokens funktionalitet i förhållande till sekretess

2.5.1.1 *Relevanta bestämmelser, m.m.*

I 8 kap. 1 § OSL framgår att uppgifter inte får röjas för enskilda eller för andra myndigheter. I 8 kap. 2 § OSL framgår att detsamma gäller mellan verksamhetsgrenar inom samma myndigheter. Vid utlämnande av sekretessbelagd uppgift har utlämnande myndighet en skyldighet att pröva utlämnandet vid varje enskilt fall utifrån regleringarna om menprövning och sekretessbrytande bestämmelser. Bedömningen blir mer strikt i händelse av att uppgifter i handlingen omfattas av omvänt skaderekvisit eller absolut sekretess. Hur detaljerad mottagaren måste vara beror på fall till fall och hur sekretessbestämmelsen är reglerad.¹⁶

2.5.1.2 *Bedömning*

Utifrån nuvarande upplägg i Ineras SDK-infrastruktur finns ingen annan kontroll och kvalitetsgranskning i samband med att en deltagare ansluter till tjänsten än uppställda skriftliga regelverk och en självdeklaration som genomförs av den anslutande deltagare.

Problem beträffande adressboken kan aktualiseras när en statlig myndighet eller en kommun eller region upprättar samma funktionsadress för olika, till varandra självständiga, verksamhetsområden hos samma deltagare.¹⁷ Som exempel torde problematiken uppstå för större statliga myndigheter med självständiga

¹⁶ Exempelvis förhållandevis vida möjligheter att inom ramen för sekretessbrytande bestämmelsen i 25 kap. 11 § 1 st. 2 p. OSL lämna hälso- och sjukvårdsinformation som omfattas av sekretess med omvänt skaderekvisit i 25 kap. 1 § OSL till annan myndighet inom samma verksamhetsområde och region. Jfr. i samma kapitel 10 § OSL undantagen till hälso- och sjukvårdssekretess där sekretess undantas för särskilda beslut inom specifika områden. Det senare exemplet torde uppställa klart större krav på utlämnande myndigheten att säkerställa dels ändamål med uppgiften, dels mottagaren.

¹⁷ Lagkommentar till 8 kap. 2 § OSL från JUNO (Norstedts Juridik), där det bland annat anges att det i ett flertal senare propositioner slagits fast att olika tillämpningar av sekretessbestämmelser medför olika verksamhetsgrenar utifrån ett sekretesshänseende. Se även prop. 2003/04:152 s. 248 f, prop. 2004/05:176, s. 55 f, prop. 2005/06:200, s. 146 f, prop. 2006/07:108, s. 43 f, prop. 2007/08:126, s. 162 f. och 202 samt JO, beslut 2019-08-30, dnr. 6547-2017.

verksamhetsgrenar och för samtliga kommuner och regioner där varje nämnd utgör självständig myndighet eller där olika utskott organiserats med särskilt verksamhetsområde. SDK är avsedd att nyttjas för sekretessärenden. Det är den utlämnande myndigheten som står risken för utlämnandet så varje enskild myndighet har att ta ställning till om de kan lämna ut sekretesskyddade uppgifter till en mottagare utifrån i adressboken angivna organisationer och verksamhetsområden.

Det räcker inte att endast kunna säkerställa rätt statlig myndighet, kommun eller region för att kunna bedöma om en handling kan lämnas ut. För att den utlämnande myndigheten ska kunna genomföra adekvata sekretessbedömningar behövs en viss detaljnivå i adressboken. Till det kan nämnas att transparensen är viktig på så sätt att tillräcklig information om respektive mottagare i adressboken behöver anges. I händelse av att en deltagare lägger in funktionsadresser på ett felaktigt sätt i adressboken kan konsekvensen bli att informationsflödet når en, utifrån sekretess och dataskydd, otillåtet bred krets av mottagare.

Till följd av avsaknaden av fastställda kontrollåtgärder utöver kodverket vid upprättande av funktionsadresser i adressboken föreligger en risk att vissa deltagare inte kommer våga använda SDK till följd av osäkerheten att rätt verksamhet är mottagare av sekretessuppgifter eller att sekretessuppgifter inte systematiskt hamnar hos fel myndighet eller verksamhet inom en viss kommun eller region. Det bör därför utredas om ytterligare kontrollåtgärder bör inrättas.

2.5.2 Adressbokens funktionalitet i förhållande till dataskyddsförordningen

Det är viktigt att deltagarna har rutiner för att hantera de personuppgifter som kan komma att skickas inom SDK

SDK är avsedd att tillämpa en alla-till-alla-lösning, det vill säga, en modell där samtliga deltagare ska kunna kommunicera med varandra. Inga begränsningar, varken avseende kommunikationsvägar mellan deltagare eller i förhållande till informationsmängd, är i dagsläget planerade. Det innebär att en deltagare inte kan styra vad för information som denna kommer att få ta emot inom infrastrukturen eller vilken annan deltagare inom infrastrukturen som har möjlighet att skicka information till denne.

Varje anslutande deltagare är skyldig att inom ramen för sitt personuppgiftsansvar säkerställa att principerna i art. 5 dataskyddsförordningen efterlevs. Regelefterlevnaden, i synnerhet principerna om laglighet, ändamålsbegränsning samt integritet och konfidentialitet, kan bli svårhanterade i händelse av att den personuppgiftsansvarige oförberedd tvingas ta emot en stor informationsmängd, inbegripet olika kategorier av personuppgifter.

Den personuppgiftsansvarige ska vidare vidta tekniska och organisatoriska säkerhetsåtgärder för den insamlade informationsmängden. Detta blir särskilt viktigt vid behandling av känsliga personuppgifter.

I normalfallet efterlevs dataskyddslagstiftningen med hjälp av krypteringar, separering av information, behörighetstilldelningar eller andra tekniska metoder som avgränsar åtkomster. Detta kan bli svårt att tillämpa i en alla-till-alla-lösning i och med att det är svårt att förutse informationsflödet och vem som ska vara behörig att ta emot informationen. Regelverket och konstruktionen i SDK medger emellertid tekniska åtgärder som avgränsar informationshanteringen inom en organisation genom funktionsadresser. Det innebär att en mottagande deltagare kan styra hur informationen kommer in och vem som tar del av den, vilket möjliggör för myndigheter att vidta säkerhetsåtgärder till viss del och därmed säkerställa sitt personuppgiftsansvar.

Vad gäller ansvaret för den information som tas emot är bedömningen att mottagaren inte rimligtvis kan anses bryta mot dataskyddsförordningen vid mottagandet av informationen eftersom ansvaret för utlämnandet ligger på den utlämnande myndigheten. Den mottagande myndigheten har emellertid ett ansvar att säkerställa lagliga och korrekta behandlingar efter det att informationen tagits emot. En avsändande deltagares bristfälliga hantering av personuppgifter kan utifrån ett sådant scenario belasta mottagaren i samband med att uppgifterna omfattas av mottagarens personuppgiftsansvar.

Ett mer långsökt problem men som ändå kan vara värt att nämna är sekretessbestämmelsen i 21 kap. 7 § OSL som förhindrar att en uppgift lämnas från en myndighet om det kan antas att uppgifter kommer behandlas i strid med dataskyddsförordningen. Om problemet med att deltagare själva lägger in information om funktionsadresser i adressbokens inte beaktas och en betydande mängd bristfälliga informationsflöden inom SDK uppmärksammas kan utlämnande myndighet tvingas till efterforskning beträffande begärande eller mottagande

myndighets tekniska lösning för att säkerställa att uppgifterna inte kommer behandlas i strid med dataskyddsförordningen. Tilliten riskerar att undergrävas varpå SDK förlorar en del av sitt syfte.

Oaktat om en felaktig funktionsadress i adressboken föreligger eller inte finns en viss risk i och med att anslutningsförfarandet sker på organisationsnivå. Ett sådant förfarande innebär att krypteringsnyckeln administreras på organisationsnivå utan hänsyn till om informationen omfattas av sekretessbestämmelser på verksamhetsnivå (till exempel att sekretessen rör uppgifter inom socialtjänsten men krypteringsnyckeln ligger hos kommunledningsförvaltningen).

2.6 Val av leverantörer

2.6.1 Sekretessfråga vid val av leverantörer

Vid val av leverantörer för accesspunkter, meddelandetjänster och meddelandeklienter är det viktigt att sekretessen beaktas och säkerställs.
--

Deltagarna kommer att behöva olika tjänster för att ansluta till och nyttja funktionerna i SDK. Dessa tjänster är bland annat accesspunkter, meddelandetjänster och meddelandeklienter.

Ett tänkbart scenario är att olika privata och offentliga deltagare erbjuder sina accesspunkter, meddelandetjänster och meddelandeklienter till anslutande deltagare som inte har kapacitet att upprätta och drifta egna sådana. Mot bakgrund av vad som tagits upp i avsnitt om informationsflödet är det viktigt att tilliten till tjänsteleverantörerna kan hållas intakt. Det är därför av yttersta vikt att de deltagare som ska nyttja dessa tjänster säkerställer leverantörernas regelefterlevnad genom kravställning och uppföljning. Om en leverantör av accesspunkt, meddelandetjänst eller meddelandeklient som inte uppfyller en tillräcklig säkerhetsnivå, inte säkerställer tillräckligt hög nivå av kryptering eller inte krypterar data även gentemot sig själv (hädanefter benämnt bristfällig tjänsteleverantör) ansluter till SDK uppstår problem för samtliga deltagare i SDK som avser att kommunicera med den deltagare som använder sig av en bristfällig tjänsteleverantör. Det finns en risk för att den deltagare som lämnar ut information i en sådan situation måste fastställa vilken accesspunktleverantör, meddelandetjänst och meddelandeklient som

används samt göra en särskild sekretessprövning inte bara i förhållande till mottagande deltagare utan även dennes accesspunktleverantör.

Den juridiska konsekvensen av att anlita bristfälliga tjänsteleverantörer är att en betydande mängd sekretesskyddade uppgifter riskerar att röjas. Förutsättningarna för tjänsteleverantörer som ska ingå i SDK måste utredas vidare i syfte att identifiera riskminimerande åtgärder.

2.6.2 Dataskyddsfrågor vid vad av leverantörer

Varje deltagare måste noggrant reglera dataskyddsregleringen mot leverantörerna av accesspunkter, meddelandetjänster och meddelandeklienter.

Varje anslutande deltagare ansvarar ytterst för att säkerställa att eventuella leverantörer uppfyller de uppställda kraven i SDK. I kraven ingår bland annat granska leverantörens olika lösningar så att frågor kopplade till dataskydd säkerställs. Ytterst torde personuppgiftsbiträdesavtalet reglera leverantörernas handlingsutrymme. Informationssäkerhetsfrågorna måste även beaktas så att anslutande deltagare i egenskap av personuppgiftsansvarig och leverantörer i egenskap av personuppgiftsbiträden säkerställer en adekvat teknisk- och organisatorisk säkerhet.

2.6.3 SDK:s kryptering i förhållande till tredjelsöverföringar

Krypteringar som tillämpas inom SDK är inte avsedda att säkerställa adekvat skyddsnivå utifrån dataskyddslagstiftning i frågan om tredjelsöverföringar.

2.6.3.1 *Relevanta bestämmelser, m.m.*

Dataskyddsförordningen utgår från att personuppgifter inte får behandlas i tredje land (länder utanför EU/EES). I särskilda undantagsbestämmelser framgår vilka förutsättningar som krävs för att överföringar till tredje land får ske. Undantagsbestämmelserna innebär att överföringar får ske till tredjeland som enligt beslut av EU-kommissionen har en så kallad adekvat skyddsnivå. Finns inget beslut

om adekvat skyddsnivå får överföring ske om personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder.¹⁸

EU-kommissionen fattade beslut den 12 juli 2016 att personuppgifter får överföras till företag i USA om företagen är anslutna till Privacy Shield. Anslutna företag ansågs till följd av Privacy Shield uppfylla kraven om en adekvat skyddsnivå.

Den 16 juli 2020 ogiltigförklarade dock EU-domstolen Privacy Shield i den så kallade Schrems II-domen.¹⁹

Till följd av Schrems II antog EDPB den 18 juni 2021 rekommendationer gällande lämpliga säkerhetsåtgärder vid överföringar av personuppgifter till tredje land.²⁰ Lämpliga tekniska åtgärder enligt EDPB:s rekommendationer består i huvudsak av kryptering.

2.6.3.2 *Bedömning*

SDK avser behandla en betydande mängd känsliga personuppgifter och i en betydande omfattning. Krypteringsåtgärderna i SDK tar sikte på att minimera risken för att sekretesskyddade uppgifter ska anses som röjda utifrån OSL. Krypteringsåtgärderna är inte avsedda att vara motståndskraftiga mot tredje lands nationella IT-kapacitet att i enlighet med utländsk lagstiftning bereda sig åtkomst till informationen. Krypteringsåtgärderna i SDK kan således inte med säker framgång åberopas som en teknisk åtgärd som möjliggör tredjelandsöverföringar.

Mot bakgrund av den informationstyp som avses behandlas i SDK och den säkerhetsmässiga enhetlighet som måste föreligga bland samtliga anslutna deltagare förutsätter DIGG att alla inblandade deltagare i SDK inte nyttjar tjänster som behandlar uppgifter i tredje land.²¹

¹⁸ Se art. 44–46 dataskyddsförordningen.

¹⁹ Mål C-311/18, Data Protection Commissioner/Maximilian Schrems och Facebook Ireland.

²⁰ EDPB:s rekommendationer 1/2020 om ytterligare åtgärder för att tillförsäkra att EU:s nivå av skydd för personuppgifter upprätthålls. EDPB (European Data Protection Board, på svenska Europeiska dataskyddsstyrelsen) består av företrädare för de nationella dataskyddsmyndigheterna och ska bidra till en enhetlig tillämpning av dataskyddsreglerna inom EU.

²¹ Resonemanget om att tilliten kan sättas ur spel vid utkontraktering till bristfällig leverantör kan likställas denna bedömning. En deltagare som genomför riskanalys vid val av accesspunktleverantör bör således riskestimera i förhållande till hela SDK.

3 Privata aktörer och konkurrens

3.1 Slutsats och/eller rekommendation

Bestämmelserna om konkurrensbegränsande offentlig säljverksamhet hindrar inte att DIGG tillhandahåller SDK. För att undvika frågetecken kring lagligheten att tillhandahålla denna offentliga säljverksamhet ser DIGG att det är en stor fördel om det finns en reglering där det framgår att DIGG ska tillhandahålla federationen.

Bestämmelserna måste dock tas i beaktande vid utformningen av SDK även om skyldigheten att tillhandahålla den framgår av reglering.

DIGG bör genomföra en behovsanalys gällande vilka behov som föreligger hos offentlig sektor att kommunicera med privata aktörer och vad för slags information som det finns behov av att utbyta. Utifrån behovsanalysen bör en fördjupad analys gällande de konkurrensrättsliga frågorna genomföras.

3.2 Inledning

Av regeringsuppdraget framgår att SDK bland annat ska kunna användas av offentlig sektor för att kommunicera med företag och andra organisationer. Exempel är privata utförare av offentligt finansierad verksamhet samt andra organisationer som offentliga verksamheter har behov av att kommunicera säkert med.

I denna del adresseras frågan kring konkurrensrättsliga bestämmelser som kan komma att aktualiseras när offentliga aktörer ägnar sig åt säljverksamhet. Enligt DIGGs bedömning är det nödvändigt att analysera dessa konkurrensfrågor oavsett om privata aktörer ska kunna ansluta till SDK eller inte för att kunna bedöma om

Om en deltagare väljer en leverantör där tredje landsöverföringar genomförs föreligger en risk att överföringen av data försvåras för samtliga deltagare.

infrastrukturen kan anses vara en säljverksamhet i lagens mening. Emellertid anser DIGG att det faktum att SDK är tänkt att kunna ansluta privata aktörer innebär att konkurrensaspekten blir extra tydlig.

De bestämmelser som bedöms vara aktuella att belysa är bestämmelser om konkurrensbegränsande offentlig säljverksamhet i 3 kap. 27–29 §§ konkurrenslagen (2008:579), de så kallade KOS-reglerna.

3.3 KOS-reglerna

KOS-reglerna kom till mot bakgrund av de problem som uppstår i samband med att offentliga aktörer bedriver konkurrensutsatt säljverksamhet, såsom undanträngningseffekter och att konkurrensen inte sker på lika villkor mellan offentliga och privata aktörer.²²

Enligt första och andra styckena 3 kap. 27 § KOS-reglerna kan staten, en kommun, en region eller en juridisk person som ägs av en offentlighetsrättslig aktör förbjudas att i en säljverksamhet tillämpa ett visst förfarande om detta snedvrider eller hämmar, eller är ägnat att snedvrیدا eller hämma, en effektiv konkurrens på marknaden. Förbud får dock inte meddelas för förfaranden som är försvarbara från allmän synpunkt.²³

²² Prop. 2008/09:231, s. 12.

²³ 3 kap. 27–29 §§ konkurrenslagen.

Av 3 kap. 27 § KOS framgår följande.

Staten, en kommun eller en region får förbjudas att i en säljverksamhet som omfattas av 1 kap. 5 § första stycket tillämpa ett visst förfarande, om detta

1. snedvrider, eller är ägnat att snedvrیدا, förutsättningarna för en effektiv konkurrens på marknaden, eller
2. hämmar, eller är ägnat att hämma, förekomsten eller utvecklingen av en sådan konkurrens.

Förbud får inte meddelas för förfaranden som är försvarbara från allmän synpunkt.

En kommun eller en region får även förbjudas att bedriva en viss säljverksamhet i fall som avses i första stycket. En sådan verksamhet får dock inte förbjudas, om den är förenlig med lag.

Ett förbud gäller omedelbart, om något annat inte bestäms.

Förbudet träffar med andra ord ett eller flera förfaranden som används inom säljverksamheten, inte själva verksamheten i sig. I denna analys utelämnas bestämmelsen i 3 kap. 27 § tredje stycket om förbud att bedriva viss säljverksamhet eftersom den bestämmelsen endast är tillämpliga på kommuner och regioner och därmed inte träffar DIGGs verksamhet som statlig myndighet.

Med säljverksamhet avses ett företag som driver verksamhet av ekonomisk eller kommersiell natur, dock inte till den del verksamheten består i myndighetsutövning.²⁴ Säljverksamheten rör den ekonomiska verksamhet som bedrivs på marknaden medan förfarandet avser de specifika villkor som tillämpas eller åtgärder som vidtas i säljverksamheten. Säljverksamheten är med andra ord *vad* som säljs och förfarandet är *hur* det säljs.²⁵

Bestämmelserna har till syfte att lösa de konkurrensproblem som uppstår vid offentlig säljverksamhet och som inte kan lösas med andra konkurrensrättsliga bestämmelser. Till exempel ska KOS-reglerna vara tillämplig på ensidiga förfaranden av en offentlig aktör som inte har en dominerande ställning på marknaden. Sådana förfaranden som typiskt sätt är tänkt att fångas upp av bestämmelserna är underprissättning, diskriminering, vägran att ge tillträde till viss infrastruktur och selektiva förfaranden. Förbud enligt KOS-reglerna bör dock inte komma i fråga för förfaranden som är en direkt och avsedd effekt av en specialreglering eller en ofrånkomlig följd av en sådan reglering. Vissa förfaranden kan också vara neutrala för konkurrensen och bör därför inte heller omfattas av KOS-reglerna. Till den kategorien kan räknas åtgärder som avser att upprätthålla service och annan infrastruktur på områden där det finns ett bristande kommersiellt utbud.²⁶

Utifrån lagparagrafens uppbyggnad sker prövningen om KOS-reglerna är tillämpliga i fyra steg:

1. Är verksamheten en ekonomisk verksamhet.
2. Är det säljverksamheten i sig eller ett visst förfarande som eventuellt är konkurrensbegränsande.

²⁴ 1 kap. 5 § konkurrenslagen.

²⁵ Lagkommentar till 3 kap. 27 § konkurrenslagen från JUNO (Norstedts juridik).

²⁶ Prop. 2008/09:231, s 33–37.

3. Snedvrider eller hämmar säljverksamheten eller förfarandet konkurrensen.
4. Är säljverksamheten förenligt enligt lag eller är förfarandet försvarbart från allmän synpunkt.

Om bedömningen är att det är en säljverksamhet enligt punkt 1 så provas sedan punkt 4 om det kan vara försvarbart från allmän synpunkt. Det finns ingen anledning att pröva ev. konkurrensbegränsning i punkt 2 och 3 om denna konkurrensbegränsning likväl är försvarbar.²⁷

3.3.2 Praxis

3.3.2.1 *Konkurrensverkets beslut gällande Helsingborgs stads tillhandahållande av kostnadsfri trådlös wifi, dnr 706/2014*

År 2012 beslutade Helsingborgs stad att erbjuda kostnadsfri wifi via surfzoner på allmän plats i centrala delar av staden. Konkurrensverket inledde en utredning för att undersöka om den tillhandahållna tjänsten stred mot KOS-reglerna. Konkurrensverket konstaterade inledningsvis att surfzonerna tillhandahölls direkt av kommunen och därmed bedrevs tjänsten av en offentlig aktör. Vad gällde frågan om kommunen bedrev en säljverksamhet som kan anses vara ett företag konstaterade Konkurrensverket att tjänsten erbjuds kostnadsfritt och frågan är om en gratistjänst kan utgöra en säljverksamhet. Konkurrensverket bedömde att så var fallet. Konkurrensverket konstaterade vidare att den datamängd som gick genom Helsingborgs wifi-nät var begränsat i förhållande till de privata operatörernas datamängder samt att det inte heller kan förutsättas att användarna skulle ha haft betalningsvilja för all den trafik som går genom kommunens nät. Den marknadsandel som Helsingborgs stad hade vid Konkurrensverkets utredning kunde därför överskatta kommunens marknadspåverkan. Slutligen ansåg Konkurrensverket att i alla fall delar av trafiken i kommunens nät var kompetensenlig och därmed i enlighet med lag. Vid en samlad bedömning ansåg Konkurrensverket att de konkurrenssnedvridande eller konkurrenshämmande

²⁷ Lagkommentar till 3 kap. 27 § konkurrenslagen från JUNO (Lexino) med hänvisningar till MD 2015:12, punkterna 63–66 och MD 2015:17 Punkterna 63–64.

effekterna av kommunens marknadspåverkan vid tiden för beslutet inte uppnått sådan betydelse som krävs för ett ingripande.

3.3.2.2 *Konkurrensverkets beslut gällande Norrsken AB gällande säljverksamhet inom fibermarknaden, dnr 795/2019*

Efter att ha mottagit ett klagomål gällande Norrsken AB inledde Konkurrensverket en utredning. Norrsken AB är ett så kallat stadsnät kluster som ägs av ett antal kommuner och kommunala stadsnät. Bolaget hyr ut kapacitetstjänster via fiber till bl.a. SVT. Konkurrensverket uppgav bland annat följande i sitt beslut. För att Norrskens eventverksamhet ska anses förenlig med lag krävs att det finns ett allmänt intresse i att bedriva denna typ av verksamhet. I praxis har det ansetts föreligga ett allmänt intresse för kommuner att tillhandahålla bredband men det är oklart om tillhandahållandet av kapacitetstjänster ska anses utgöra ett allmänt intresse eftersom dessa tjänster är mer förädlade. Konkurrensverket hänvisade till den så kallade värdekedjan inom fiber- och bredbandstjänster som har definierats av Post- och Telestyrelsen (PTS) och som är enligt följande:

1. Passivt nät (infrastruktur och svartfiber).
2. Aktivt nät (transmission eller kapacitetstjänster, svartfibern aktiveras med hjälp av aktiv utrustning).
3. Kommunikationsnivå (dirigerar och administrerar det aktiva nätet. Erbjuder tjänsteabonnemang via plattform).
4. Tjänster (tjänsteleverantörer ser till att konsumenter får tillgång till tjänster som internet, telefoni, tv).

Enligt Konkurrensverkets bedömning är det endast verksamhet på den första nivån som tydligt har ett allmänintresse. För mer förädlade tjänster är det tveksamt om ett sådant intresse föreligger. Konkurrensverket fann att det inte var motiverat med en fortsatt utredning då det inte har framkommit några tydliga tecken på att konkurrensen snedvridits eller hämmats.

3.4 Bedömning

3.4.1 Är SDK en ekonomisk verksamhet som utgör ett företag

Med hänsyn till den vidsträckta definitionen av vad som utgör företag i konkurrensrättslig mening är bedömning att SDK bör ses som en säljverksamhet hos DIGG, oavsett vilken finansieringsmodell som väljs.

Vidare är bedömningen att om en deltagande myndighet utvecklar sin egen accesspunkt och erbjuder denna tjänst till andra deltagande myndigheter så kommer även det att ses som säljverksamhet. Vid en sådan situation inom kommunal sektor kan även frågor om den kommunala kompetensen aktualiseras.

För att KOS-reglerna ska vara tillämpliga måste det vara fråga om en säljverksamhet som utgör företag och som bedrivs i staten, kommunen eller regionen eller i en särskild juridisk person i vilken staten, kommunen eller regionen har ett dominerande inflytande. Till säljverksamhet räknas inte bara försäljning utan även andra utbudsverksamheter, exempelvis uthyrning. Det behöver inte föreligga något vinstsyfte för att verksamhetens ska anses vara ett företag, utan det som är avgörande är om verksamheten utövas på en konkurrensutsatt marknad.²⁸

Begreppet "företag" är ett EU-rättsligt begrepp och ska tolkas vidsträckt och träffar i stort sett varje verksamhet i av ekonomisk natur som inte utgör myndighetsutövning. Det spelar ingen roll om verksamheten utövas i offentlig eller privat regi. Att verksamheten bedrivs utan vinstsyfte spelar heller ingen roll om den utövas i konkurrens med andra verksamheter som drivs i vinstsyfte. Även ideell och religiös verksamhet kan utgöra företag i konkurrensrättslig mening. För att en verksamhet ska anses utgöra företag krävs emellertid att någon form av ekonomisk verksamhet bedrivs med viss varaktighet. Dock har verksamheter som bedriver nyttigheter med ett icke-ekonomiskt syfte inte ansetts som företag trots att de haft viss säljverksamhet. Exempel är sjukvård och utbildning.²⁹

²⁸ Prop. 2008/09:231, s. 34–35.

²⁹ Lagkommentar till 1 kap. 5 § konkurslagen från JUNO (Norstedts juridik, kapitel 1.1 och 1.4).

3.4.1.1 *Slutsats*

Frågan är om DIGG kan anses tillhandahålla en säljverksamhet via SDK samt om denna verksamhet är av ekonomisk eller kommersiell natur (det vill säga, ett företag) i konkurrensrättslig mening.

Via SDK kommer DIGG att erbjuda en infrastruktur för säker digital kommunikation för offentlig sektor. Om DIGG kommer att ta betalt av deltagande organisationer eller inte är ännu inte beslutat. Såsom framgår ovan så är det inte nödvändigt att det finns ett vinstsyfte eller att verksamheten erbjuds mot betalning för att det ska anses vara en säljverksamhet, utan bedömningen utgår från om DIGG bedriver säljverksamhet i konkurrens med andra eller hindrar att en marknad kan utvecklas inom området.

Den kan inte uteslutas att SDK kan ses som en tjänst som konkurrerar med andra tjänster inom elektroniska kommunikationstjänster och plattformar eller riskerar att påverka en möjlighet för andra aktörer att slå sig in på en marknad med liknande tjänster som SDK erbjuder. Ser man till den så kallade värdekedjan så är det troligt att SDK ska ses som en tjänst på nivå tre eller fyra. För att med större säkerhet kunna uttala sig om eventuella konkurrenter måste den relevanta marknaden fastställas. Bedömningen av vad som utgör ett företag kan emellertid göras separat i ett första steg för att sedan pröva de övriga rekvisiten som ställs upp i lagrummet.

Bedömningen blir därför, med hänsyn till den vidsträckta definitionen av vad som utgör företag i konkurrensrättslig mening, att SDK bör ses som säljverksamhet för både DIGG och deltagande myndigheter som eventuellt väljer att sälja accesspunktstjänster.

3.4.2 Är förfarandet försvarbart från allmän synpunkt

Om det framgår tydligt via lagstiftning att DIGG ska tillhandahålla SDK samt hur federationen ska tillhandahållas är bedömningen att säljverksamheten via SDK med största sannolikhet anses vara försvarbart från allmän synpunkt och därmed inte träffas av bestämmelserna om konkurrensbegränsande offentlig säljverksamhet.

Det är viktigt att DIGG utformar SDK på ett sätt som inte hämmar eller snedvrider, eller riskerar att hämma eller snedvrída, konkurrensen mer än nödvändigt.

Konkurrensbegränsande förfaranden får inte förbjudas om förfarandet anses vara försvarbart från allmän synpunkt.³⁰ Om ett förfarande anses vara försvarbart från allmän synpunkt finns det ingen anledning att pröva de övriga stegen enligt KOS-reglerna gällande om förfarandet i sig är konkurrensbegränsande eftersom (det konkurrensbegränsande) förfarandet anses tillåtet oavsett.

För att avgöra om ett förfarande är försvarbart från allmän synpunkt måste man först pröva vad för rättsliga förutsättningar som gäller och undersöka om förfarandet strider mot lag, annan författning eller andra bindande direktiv. Om de konkurrenssnedvidande effekterna är en direkt eller avsedd verkan av lagstiftningen bör dessa inte omfattas av KOS-reglerna. Även motiven bakom de konkurrenssnedvidande effekterna ska vägas in i bedömningen. Motiv som grundas på det allmännas behov att verksamheten bedrivs bör anses försvarbara. Om motiven är interna och handlar om aktörens egenintresse anses förfarandet inte vara försvarbart. I avvägningen mellan konkurrensintresset och ett annat allmänt intresse bör man beakta om det finns ett annat sätt att tillgodose det allmännas behov än genom det konkurrensskadliga beteendet. Finns det andra vägar att tillgodose det allmänna intresset kan beteendet inte anses försvarbart.³¹

³⁰ 3 kap. 27 § andra stycket konkurrenslagen.

³¹ Prop. 2008/09:231, s. 37–38.

3.4.2.1 *Slutsats*

Med hänsyn till att DIGG enligt regeringsuppdraget har fått som uppdrag att tillhandahålla SDK, och under förutsättning att det senare kommer att framgå av författning att DIGG ska hålla infrastrukturen och hur den ska tillhandahållas, är bedömningen att säljverksamheten och förfarandena för att tillhandahålla säljverksamheten kommer att kunna bedömas vara försvarbar från allmän synpunkt.

Som statlig myndighet kan DIGG endast förbjudas att tillämpa vissa förfaranden inom en säljverksamhet men inte förbjudas att bedriva själva verksamheten. Den ovan angivna praxisen gällande bredbandstjänster är därför inte fullt ut applicerbar för denna situation i och med att praxisen rör kommuners lagenliga rätt att bedriva viss verksamhet.

Likväl kan en eller flera förfaranden som DIGG tillämpar anses vara otillåtna om de har utformats på ett sätt som begränsar konkurrensen mer än nödvändigt och inte är en direkt eller avsedd verkan av lagstiftningen. I detta hänseende kan praxisen som refererats bli relevant i viss utsträckning för att bedöma om förfarandet är tillåtet.

DIGG är alltså inte fri att utforma SDK hur som helst även om myndigheten har i uppdrag att tillhandahålla den. DIGG måste ha med den konkurrensrättsliga aspekten i utformningen av regler, ramverk och finansieringsmodell.

Denna bedömning omfattar inte det fall att en deltagande myndighet väljer att säja accesspunktstjänster eller andra tjänster inom SDK till andra deltagare. För att undantaget ska vara tillämpligt i det fallet måste den deltagande myndigheten ha i uppdrag att utföra denna tjänst eller att det ska anses falla inom den kommunala kompetensen att tillhandahålla denna tjänst.

3.4.3 Är det säljverksamheten eller ett specifikt förfarande som ev. är konkurrensbegränsande

Eftersom bedömningen är att säljverksamheten kan anses vara försvarbar från allmän synpunkt behöver ingen bedömning göras om förfarandet kan snedvrída eller hämma konkurrensen.

3.4.4 Resulterar säljverksamheten eller förfarandet en snedvrídning eller hämmande av konkurrensen

Eftersom bedömningen är att säljverksamheten kan anses vara försvarbar från allmän synpunkt behöver ingen bedömning göras om förfarandet kan snedvrída eller hämma konkurrensen.

4 Upphandling

4.1 Slutsats och/eller rekommendation

SITUATION	BEDÖMNING
Kommuns eller regions anslutning till SDK	Kan vara upphandlingspliktig
Statlig myndighets anslutning till SDK	Ej upphandlingspliktig
accesspunktsoperatörers eller annan tredjepartsleverantörs anslutning till SDK	Sannolikt inte upphandlingspliktig
Deltagarens anlitande av accesspunktsoperatör eller annan tredjepartsleverantör	Kan vara upphandlingspliktig

4.2 Inledning

Denna del av den rättsliga analysen behandlar upphandlingsrättsliga förutsättningar för SDK. I analysen redogörs huvudsakligen för frågor om upphandlingsskyldighet samt upphandlingsrättsliga aspekter som kan komma att ha betydelse för SDK.

Den upphandlingsrättsliga analysen har fokuserat på att belysa de relationer som kan komma att uppstå mellan olika aktörer ur ett upphandlingsrättsligt perspektiv med tyngdpunkten vid tre centrala moment:

- Deltagarnas tillträde till och användning av SDK.
- Anskaffning av eventuella tredjepartstjänster.
- Eventuell underleverantörsroll.

Inom ramen för SDK kan ett flertal anslutningsavtal komma att ingås (beskrivningen utgår från nuvarande lösning men som framgår av delrapporten under avsnitt 4.5 om avtalsmodell behöver det utredas exakt vad förslags

avtalsmodell som ska finnas om det är så att skyldigheten att tillhandahålla SDK framgår av författning). Plattformansvarig ansvarar för att godkänna accesspunktsoperatörer och ansluta dessa till plattformen. Plattformansvarig ansvarar vidare för att ansluta eventuella federationer till plattformen och tecknar härvid anslutningsavtal med en federationsägare (för det fall plattformansvarig inte samtidigt är federationsägare). För anslutning av deltagare till infrastrukturen kommer anslutningsavtal att ingås mellan federationsägaren och respektive deltagare. Anslutningsavtalen kommer sannolikt att innehålla bland annat villkor för tillträde till SDK och användning av densamma, men kommer sannolikt även att omfatta tillhandahållande av olika stödtjänster (vidare är det inte otänkbart att tillträdet till SDK i sig kan anses utgöra tillhandahållande av en tjänst, se nedan).

Utöver anslutningsavtalen kommer sannolikt ett flertal renodlade tjänsteavtal att ingås mellan olika aktörer inom ramen för SDK. Ovannämnda accesspunktsoperatörer kommer att tillhandahålla accesspunktstjänster till deltagare och härutöver kan förväntas att de tjänster som tillhandahålls av tredjepartsleverantörer kommer att regleras i separata tjänsteavtal. Vidare kommer en eventuell underleverantör sannolikt att tillhandahålla olika typer av tjänster till eller på uppdrag av federationsägaren.

SDK utgör en mjukvarubaserad lösning för kommunikation i befintliga fysiska nätverk, en digital plattform där tillgång och innehåll är reglerat (bland annat genom olika krav för att säkerställa tillit, säker överföring av information, behörighetskrav m.m.). SDK är dock inte i sig vare sig ett fysiskt nätverk för kommunikation eller en kommunikationstjänst, utan kan snarare beskrivas som en reglerad samverkan, baserad på bland annat ett tillitsramverk.

4.3 Tillämpliga bestämmelser, m.m.

4.3.1 Upphandlingspliktiga anskaffningar, särskilt om kontraktsbegreppet och tilldelning av kontrakt

4.3.1.1 Vem är skyldig att upphandla?

Som huvudregel ska den offentliga sektorns anskaffningar konkurrensutsättas i enlighet med upphandlingslagstiftningen. Av 1 kap. 2 § lagen (2016:1145) om

offentlig upphandling (LOU) följer att lagen är tillämplig vid upphandling som genomförs av en upphandlande myndighet. Med upphandling avses de åtgärder som vidtas i syfte att anskaffa varor, tjänster eller byggtreprenader genom tilldelning av kontrakt.

Med upphandlande myndighet avses enligt definitionen i 1 kap. 22 § LOU en statlig eller kommunal myndighet. Med myndighet jämställs såväl beslutande församlingar i kommuner och regioner som s.k. offentligt styrda organ, samt sammanslutningar av dessa typer av aktörer.

Med offentligt styrt organ avses enligt definitionen i 1 kap. 18 § LOU en sådan juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och (i) som till största delen är finansierad av staten, en kommun, en region eller en upphandlande myndighet, (ii) vars verksamhet står under kontroll av staten, en kommun, en region eller en upphandlande myndighet, eller (iii) i vars styrelse eller motsvarande ledningsorgan mer än halva antalet ledamöter är utsedda av staten, en kommun, en region eller en upphandlande myndighet.

Som utgångspunkt för analysen kan konstateras att såväl DIGG som de offentliga aktörer som kommer att ansluta sig till SDK och använda sig av eventuella tjänster utgör upphandlande myndigheter som är skyldiga att tillämpa upphandlingslagstiftningen för de anskaffningar som görs som faller inom lagstiftningens tillämpningsområde.

4.3.1.2 Vilken typ av kontrakt omfattas?

Av LOU:s inledande definition av vad som utgör offentlig upphandling följer att ett antal förutsättningar ska vara uppfyllda för att en viss åtgärd, till exempel ett ingående av avtal om tjänster, ska omfattas av lagen.

En eller flera upphandlande myndigheter ska genomföra en anskaffning av varor, tjänster eller byggtreprenader. Denna anskaffning ska ske genom tilldelning av ett kontrakt till en leverantör som har valts ut av den eller de upphandlande myndigheterna.

Definitionen av ett offentligt kontrakt följer av 1 kap. 15 § LOU, vari det framgår att det ska röra sig om ett skriftligt avtal med ekonomiska villkor som (i) ingår

mellan en eller flera upphandlande myndigheter och en eller flera leverantörer och (ii) avser leverans av varor, tillhandahållande av tjänster eller utförande av byggtreprenad.

Begreppet anskaffning ska förstås i vid mening som att den upphandlande myndigheten får tillgång till fördelarna av varorna, tjänsterna eller byggtreprenaderna. För att det ska vara fråga om en anskaffning krävs dock att det rör sig om en utväxling av prestationer av något slag. Ren finansiering av verksamhet utan krav på motprestation, gåvor, bidrag och liknande åtgärder omfattas inte av anskaffningsbegreppet.³²

Av EU-domstolens praxis följer att för att det ska föreligga ett sådant avtal med ekonomiska villkor som omfattas av kontraktsbegreppet krävs att en leverantör, i utbyte mot ersättning, tillhandahåller varor, tjänster eller byggtreprenader som är av direkt ekonomiskt intresse för den upphandlande myndigheten. Vidare ska det uppstå (ömsesidiga) skyldigheter av rättsligt bindande karaktär. Ersättningen är vid detta av central betydelse – om avtalet inte omfattar någon skyldighet för den upphandlande myndigheten att utge ersättning eller någon annan slags motprestation med ett ekonomiskt värde (det måste inte nödvändigtvis röra sig om en regelrätt betalning med pengar, även andra former av ersättning är tänkbara) rör det sig inte om ett kontrakt i upphandlingsrättslig mening.³³

I förarbetena till LOU framhålls att skälet för anskaffningen inte är avgörande för om det är fråga om upphandling eller inte samt att det saknar betydelse om leverantörens motprestation kommer den upphandlande myndigheten eller tredje man till godo. Den upphandlande myndigheten måste alltså inte ha syftet att själv tillgodogöra sig det som anskaffas. Som exempel nämns att det är fråga om upphandling när en inköpscentral vidtar åtgärder för att ingå ett ramavtal eller inrätta ett dynamiskt inköpssystem som ska användas av andra upphandlande myndigheter för senare anskaffningar, eller när en upphandlande myndighet agerar i en upphandling som ombud för en annan upphandlande myndighet.³⁴

³² Skäl 4, andra stycket i Europaparlamentets och rådets direktiv 2014/24/EU om offentlig upphandling.

³³ EU-domstolens mål nr C-367/19, Tax-Fin-Lex, C-51/15, Remondis och C-451-08, Helmut Müller.

³⁴ Prop. 2015/16:195, s 933.

En särskild fråga som ska uppmärksammas i förhållande till det upphandlingsrättsliga kontraktsbegreppet är att avtal mellan statliga myndigheter inte anses utgöra offentliga kontrakt enligt upphandlingslagstiftningen. Det följer av Högsta förvaltningsdomstolens (HFD) avgörande i HFD 2021 ref. 35 att köp mellan statliga myndigheter under regeringen inte omfattas av det upphandlingsrättsliga regelverket, bland annat mot bakgrund av att myndigheterna ingår i samma juridiska person (staten) och att de inte kan ingå civilrättsligt bindande avtal med varandra. HFD framhöll att det följer av EU-domstolens praxis att det upphandlingsrättsliga regelverket är tillämpligt endast med avseende på avtal som ingås mellan en upphandlande myndighet och en från den myndigheten fristående fysisk eller juridisk person. Inom en och samma juridiska person kan det inte, på det sätt som krävs, uppkomma rättsligt bindande skyldigheter vars fullgörande går att uppnå genom rättsliga åtgärder.

Detta innebär att eventuella anskaffningar mellan statliga myndigheter inom ramen för tillhandahållandet eller användningen av SDK inte omfattas av upphandlingsskyldighet eftersom det ur ett upphandlingsrättsligt perspektiv inte kan anses röra sig om offentliga kontrakt.

I detta sammanhang ska också för fullständighetens skull noteras att om den aktör som ska tillhandahålla de nyttigheter som den upphandlande myndigheten är i behov av har en ensamrätt enligt lag, det vill säga, om den upphandlande myndigheten inte har möjlighet att välja sin avtalspart, kan det argumenteras för att det inte rör sig om ett kontrakt i upphandlingsrättsligt hänseende. Vidare följer uttryckligen av 3 kap. 10 § LOU att lagen inte gäller för ett tjänstekontrakt som en upphandlande myndighet tilldelar en annan upphandlande myndighet som på grund av lag eller annan författning har ensamrätt att utföra tjänsten, se vidare i avsnitt om övriga särskilda undantag nedan (en sådan situation med legal ensamrätt ska dock inte förväxlas med situationen att det av någon annan anledning endast finns en aktör på marknaden).

Mot ovanstående bakgrund får såväl eventuella anskaffningar mot ersättning som görs av DIGG i syfte att upprätta och driva SDK, från federationsägare (om annan aktör än DIGG) eller från federationsoperatören eller annan leverantör av tjänster, anses utgöra offentliga kontrakt. Vidare omfattas sannolikt eventuella tjänster som anskaffas av de upphandlande myndigheter som ska ansluta sig till SDK av kontraktsbegreppet förutsatt att ersättning för användningen av tjänsterna utgår (som utvecklas nedan kan dessa kontrakt dock vara undantagna enligt något av de

undantag LOU innehåller avseende anskaffningar mellan upphandlande myndigheter). Tillhandahållande av tjänster som görs vederlagsfritt, det vill säga utan krav på ersättning, är dock sannolikt inte att betrakta som offentliga kontrakt.

4.3.1.3 *Tilldelning av kontrakt*

Vad som avses med termen tilldelning av kontrakt definieras varken i LOU eller i det bakomliggande EU-direktivet, direktiv 2014/24/EU (LOU-direktivet). Med tilldelning av kontrakt avses enligt förarbetena till LOU den upphandlande myndighetens beslut i fråga om val av leverantör. För att det ska vara fråga om upphandling krävs det ett inslag av selektivitet, det vill säga att en eller flera leverantörer väljs ut av den upphandlande myndigheten. Detta jämförs med situationer där samtliga leverantörer som uppfyller vissa villkor har rätt att utföra en bestämd uppgift utan selektivitet, till exempel vid valfrihet för kunden och system med servicecheckar. Sådana situationer bör enligt skälen till LOU-direktivet inte ses som upphandling, utan enbart som auktorisationssystem.³⁵

4.3.2 Potentiellt tillämpliga undantag

Beroende på hur SDK kommer att tillhandahållas och vilka deltagare som är inblandade så kan Teckal – och Hamburgundantagen bli tillämpliga.

Det är inte troligt att andra undantag i upphandlingslagstiftningen är tillämpliga.

4.3.2.1 *Kontrakt avseende allmänna kommunikationsnät och elektroniska kommunikationstjänster (det s.k. teleundantaget)*

Enligt 3 kap. 6 § LOU är lagen inte tillämplig vid en upphandling eller en projektävling som huvudsakligen syftar till att ge en upphandlande myndighet möjlighet att

³⁵ Prop. 2015/16:195, s 933–934 och skäl 4 i LOU-direktivet.

1. tillhandahålla eller driva ett allmänt elektroniskt kommunikationsnät, eller
2. för allmänheten tillhandahålla en elektronisk kommunikationstjänst.

Bestämmelsen hänvisar i fråga om begreppen "*allmänt elektroniskt kommunikationsnät*" och "*elektronisk kommunikationstjänst*" till lagen (2022:482) om elektronisk kommunikation (LEK).³⁶

Undantaget omfattar bland annat publika telenät, innefattande bredbandsnät, och teletjänster, nät för överföring av tv- och radiosignaler samt nätverk för kabel-tv och motiveras bl.a. av att de upphandlande myndigheter som är verksamma inom något av dessa områden agerar på en marknad som sedan sektorns avreglering är utsatt för ett särskilt konkurrenstryck och att de därmed kan antas genomföra sina inköp affärsmässigt.

För att undantaget ska vara tillämpligt i förhållande till en viss anskaffning förutsätts dock först och främst att det överhuvudtaget är fråga om ett kontrakt som huvudsakligen syftar till att ge den upphandlande myndigheten möjlighet att tillhandahålla sådana nät eller tjänster som avses i bestämmelsen. I litteraturen har angetts att det i enlighet med vad som gäller enligt övriga bestämmelser i LOU och principer för avgörande av för vilken verksamhet upphandling sker, ska göras en bedömning enligt den så kallade överviktsprincipen och att undantaget således är tillämpligt under förutsättning att kontraktet huvudsakligen är avsett för den verksamhet som anges i bestämmelsen.

Därutöver krävs att kontraktet avser tillhandahållande eller drift av allmänna elektroniska kommunikationsnät eller tillhandahållande av elektroniska kommunikationstjänster för allmänheten.

³⁶ Lagen 2003:389 in elektronisk kommunikation har upphävts och ersatts av lagen 2022:482 om elektronisk kommunikation. Med den nya lagen har det tidigare begreppet "*allmänt kommunikationsnät*" ersatts av begreppet "*allmänt elektroniskt kommunikationsnät*". Detta innebär inte någon ändring i sak. Definitionen av elektronisk kommunikationstjänst har i den nya lagen fått en något vidare innebörd. Därmed vidgas undantaget från lagens tillämpningsområde något, se prop.2021/22:136, s. 122–124, 551.

"Elektronisk kommunikationstjänst" definieras i 1 kap. 7 § LEK som en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som är en

- 1 internetanslutningstjänst,
- 2 interpersonell kommunikationstjänst, eller
- 3 tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio.

Elektroniskt kommunikationsnät definieras som ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.

Som angetts ovan avser undantaget i första hand olika typer av publika telenät och teletjänster, innefattande exempelvis bredbandsnät, samt nät för överföring av tv- och radiosignaler m.m. Bedömningen mot bakgrund av detta är att det de fysiska nätverken och tillhandahållandet av kommunikationstjänster som är centralt för undantaget.

SDK kan närmast sägas utgöra en innehållsreglering och behörighetsstyrning för säker kommunikation på befintliga nätverk snarare än en sådan typ av etablering av infrastruktur som omfattas av undantagets tillämpningsområde. Det kan härutöver ifrågasättas om det rör sig om en allmänt tillgänglig infrastruktur eller om ett slutet system huvudsakligen avsett för anslutna deltagare (till skillnad från exempelvis ett offentligt bredbandsnät i en kommun eller andra typer av öppna kommunikationsnät).

I Post- och telestyrelsens vägledning avseende LEK noteras att även ett nät med få användare anses utgöra ett allmänt kommunikationsnät om det erbjuds till en vidare krets. Om kommunikationsnätet dock endast erbjuds till en på förhand bestämd krets av användare, till exempel på grund av ett annat kontraktuellt förhållande, kan nätet däremot inte anses vara allmänt. Mycket talar för att SDK inte ska betraktas som ett sådant allmänt kommunikationsnät som omfattas av LEK och det aktuella undantaget.

4.3.2.2 *Upphandling mellan offentliga aktörer – Teckal- och Hamburgundantagen*

Teckalundantaget

Av 3 kap. 11–16 §§ LOU följer att lagen inte är tillämplig om det rör sig om en intern upphandling, det s.k. Teckalundantaget (alternativt undantaget för inhouse-upphandling).

Undantaget är, något förenklat, tillämpligt i situationer då den upphandlande myndigheten har en kontroll över sin en avtalspart som motsvarar den kontroll som myndigheten utövar över sin egen förvaltning (det så kallade kontrollkriteriet) och motparten dessutom bedriver huvuddelen (mer än 80 procent) av sin verksamhet tillsammans med den upphandlande myndigheten (det så kallade verksamhetskriteriet). Ytterligare en förutsättning är att det inte får finnas något direkt privat ägarintresse i motparten.

Undantaget är tillämpligt även om den upphandlande myndigheten utövar kontrollen gemensamt med andra upphandlande myndigheter. Vidare kan undantaget tillämpas omvänt, i situationer då det är den upphandlande myndigheten som står under motpartens kontroll, och horisontellt mellan två eller flera fristående enheter som kontrolleras av samma upphandlande myndighet. Båda dessa senare situationer förutsätter att kontrollen utövas av en upphandlande myndighet, det vill säga gemensam kontroll är inte tillräckligt.

Det är möjligt att vissa anskaffningar som kan komma att göras inom ramen för tillhandahållandet av SDK kan omfattas av Teckalundantaget (beroende på vilka parter som är involverade). Det är exempelvis tänkbart att om en kommun eller region anskaffar en accesspunktstjänst via en Accesspunktsoperatör som de kommunala eller regionala myndigheterna gemensamt utövar kontroll över så kan den anskaffningen omfattas av undantaget. Det kan dock konstateras att Teckalundantaget inte kan tillämpas i förhållande till eventuella anskaffningar mellan DIGG och en aktör som kommun eller region utöver gemensam kontroll över eller mellan olika statliga och kommunala myndigheter.

Vidare måste beaktas att verksamhetskriteriet innebär att huvuddelen av verksamheten måste bedrivas tillsammans med den upphandlande myndighet som utövar kontrollen.

Hamburgundantaget

Av 3 kap. 17 § LOU följer att lagen inte gäller för upphandling mellan två eller flera upphandlande myndigheter, förutsatt att

- upphandlingen syftar till att upprätta eller reglera formerna för ett samarbete mellan myndigheterna som ska säkerställa att de offentliga tjänster som myndigheterna ska utföra tillhandahålls för att uppnå myndigheternas gemensamma mål
- samarbetet styrs endast av överväganden som hänger samman med allmänintresset
- myndigheterna på den öppna marknaden utövar mindre än 20 procent av den verksamhet som berörs av samarbetet
- samarbetet inte får leda till att ett privat företag gynnas i förhållande till sina konkurrenter.

Det ska i sammanhanget noteras särskilt att det i förarbetena till bestämmelsen framhålls att formuleringen ”*upprätta eller reglera formerna för ett samarbete*” innebär att det finns utrymme för en upphandlande myndighet att ansluta sig i efterhand till ett redan existerande samarbete mellan andra myndigheter.³⁷ Samtliga deltagande upphandlande myndigheter måste således inte ha varit involverade i samarbetet från början.

Bedömning är att det är möjligt att ett eventuellt samarbete mellan DIGG och en aktör som skulle få ta över visst ansvar inom infrastrukturen i egenskap av federationsoperatör eller annan slags underleverantör skulle kunna struktureras på ett sådant sätt att det omfattas av Hamburgundantaget, förutsatt att det de facto rör sig om ett samarbete och inte att DIGG ”anlitar” en aktör som får i uppdrag av DIGG att agera federationsoperatör eller annan slags underleverantör. Se vidare nedan.

³⁷ Prop. 2015/16:195, s. 966.

4.3.2.3 Övriga särskilda undantag – Särskilt om ensamrätt

Det ska inte uteslutas att det finns andra undantag från upphandlingsskyldighet som kan komma att aktualiseras, beroende på hur SDK närmare utformas och kommer att tillhandahållas.

Ett undantag som bör framhållas i sammanhanget är bestämmelsen i 3 kap. 10 § LOU enligt vilken lagen inte ska tillämpas på tjänstekontrakt som en upphandlande myndighet tilldelar en annan upphandlande myndighet som på grund av lag eller annan författning har ensamrätt att utföra tjänsten.

Undantaget är avsett att tillämpas i fall då en upphandlande myndighet (eller en sammanslutning av upphandlande myndigheter) är den enda som får tillhandahålla en viss tjänst eftersom de har en ensamrätt enligt lagar eller andra offentliggjorda författningar. Det ska understrykas att dessa lagar eller författningar måste vara förenliga med fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

Detta undantag innebär att om DIGG skulle göras till ansvarig myndighet för SDK och genom lag eller författning tilldelas en ensamrätt att tillhandahålla SDK till deltagande upphandlande myndigheter (innefattande statliga myndigheter, regioner, kommuner och eventuella offentligt styrda organ som jämställs med myndigheter) skulle själva tillhandahållandet av SDK och eventuella tjänster som DIGG tillhandahåller andra upphandlande myndigheter sannolikt inte omfattas av upphandlingsskyldighet för dessa myndigheter. Förutsättningarna för en sådan reglering och konsekvenserna bör dock utredas närmare.

4.4 Bedömning

Detta avsnitt innehåller en upphandlingsrättslig analys i förhållande till centrala aspekter av SDK såsom deltagarnas tillträde till och användning av infrastrukturen och anskaffning av eventuella tredjepartstjänster.

4.4.1 Deltagarnas tillträde till och användning av SDK

Att ansluta sig till SDK mot ersättning bedöms vara en anskaffning som omfattas av upphandlingsplikt. Statliga myndigheter behöver dock inte upphandla tjänsten att ansluta sig till SDK eftersom det inte föreligger upphandlingsplikt mellan statliga myndigheter.

Att anskaffa tjänster som krävs för att kunna utbyta information inom federationen från en kommersiell leverantör bedöms vara upphandlingspliktiga anskaffningar.

En första fråga är huruvida de deltagare som är upphandlande myndigheter kan komma att behöva genomföra en eller flera offentliga upphandlingar för att ansluta sig till SDK.

Det kan övervägas om SDK utgör en tjänst eller om det rör sig om något annat. Att ingå avtal om att följa en gemensam teknisk standard för kommunikation och i övrigt acceptera de villkor som gäller för att verka inom en federation ansluten till plattformen eller att ansluta sig till ett tillitsramverk utgör inte nödvändigtvis en anskaffning av en eller flera tjänster. Som angetts ovan är en av förutsättningarna för att det, ur ett upphandlingsrättsligt perspektiv, ska vara fråga om ett kontrakt att en leverantör tillhandahåller en tjänst som är av direkt ekonomiskt intresse för den upphandlande myndigheten.

Övervägande skäl talar dock för att anslutningen till infrastrukturen, det vill säga att deltagarna tillhandahålls möjlighet att utbyta information med varandra och tillgodogör sig olika typer av tjänster i samband med detta, bör betraktas som ett tjänsteavtal i upphandlingsrättslig mening och att deltagarna således anskaffar en tjänst från federationsägaren. Om deltagarna betalar en avgift för att ansluta till SDK och/eller för att få utnyttja de tjänster som tillhandahålls inom ramen för SDK kommer det sannolikt att uppkomma ett eller flera upphandlingspliktiga tjänstekontrakt. De deltagare som är upphandlande myndigheter kommer därmed att behöva konkurrensutsätta tjänsterna såvida det inte finns något tillämpligt undantag i upphandlingslagstiftningen. I vart fall tillhandahålls en rad olika typer av tjänster (plattformstjänster, federationstjänster, supporttjänster m.m.) inom ramen för SDK.

DIGG kommer att vara federationsägare för SDK. Detta medför sannolikt att DIGG är att betrakta som leverantör i förhållande till deltagarna, varför

upphandlingsskyldighet inte torde uppkomma för de deltagare som är statliga myndigheter (jfr HFD 2021 ref. 35) men däremot eventuellt för regioner, kommuner och offentligt styrda organ.

Om tillträdet till SDK (det vill säga. deltagarnas anslutning till infrastrukturen) och användningen av de tjänster som omfattas av tillhandahållandet är avgiftsfritt för deltagarna är bedömning att det inte uppkommer något upphandlingspliktigt kontrakt i detta led, vare sig i förhållande till statliga myndigheter eller andra upphandlande myndigheter.

I förhållande till ovan kan sammanfattningsvis följande upphandlingsrättsliga förutsättningar noteras:

- En avgörande fråga är om tillträdet till, och användningen av, SDK kommer att vara kostnadsfritt för deltagarna eller avgiftsfinansierat. Om SDK tillhandahålls kostnadsfritt aktualiseras sannolikt inte upphandlingsreglerna överhuvudtaget för de deltagare som vill få tillträde (innefattande statliga myndigheter, kommuner/regioner och offentligt styrda organ som jämföras med upphandlande myndigheter).
- Om tillträdet till SDK (innefattande de olika tjänster som tillhandahålls av DIGG) är avgiftsfinansierat kan tillträdet och användningen komma att vara upphandlingspliktigt för deltagande upphandlande myndigheter. Statliga myndigheters anslutning till SDK torde dock undantas upphandlingsreglernas tillämpning, eftersom avtal mellan statliga myndigheter och DIGG inte utgör kontrakt i upphandlingsrättsligt hänseende.

4.4.2 Anskaffning av eventuella tredjepartstjänster

Som angetts ovan kan olika typer av tjänsteleverantörer komma att vara anslutna till plattformen eller infrastrukturen. En sådan tjänsteleverantör är accesspunktsoperatören, som godkänns av plattformsansvarig enligt regelverket för plattformen och därefter ansluts till plattformen, varefter federationsägaren ansluter accesspunktsoperatören till federationen. Även andra typer av tjänsteleverantörer kan komma att verka inom ramen för infrastrukturen och tillhandahålla tjänster till deltagare. Vidare kan deltagare komma att behöva

anskaffa tjänster från externa leverantörer, till exempel för anpassning av den interna IT-miljön inför anslutning till SDK.

En ren godkännandeprocess, det vill säga, att DIGG eller någon annan aktör enbart godkänner och "släpper in" en leverantör i SDK kan inte ses som en anskaffning från DIGGs sida. Vidare har noterats ovan att om alla leverantörer, eller i förekommande fall alla leverantörer som uppfyller uppställda krav, får ingå ett visst avtal bör förfarandet närmast ses som ett slags auktorisationssystem eller jämföras med ett slags certifieringsförfarande och inte betraktas som ett ingående av kontrakt.

Anslutning av tredjepartsleverantörer kommer således inte i sig att aktualisera upphandlingsskyldighet, förutsatt att det kan jämföras med ett auktorisationssystem eller en certifiering av leverantörerna. DIGG kommer i egenskap av plattformsansvarig och/eller federationsägare endast att ha en samordnande funktion och ansvara för tekniska standarder och krav m.m. samt säkerställa att anslutna tjänsteleverantörer är "godkända" att leverera tjänster och verka inom ramen för SDK. Eventuell upphandlingsplikt uppkommer först i nästa led, när deltagarna ska anskaffa tjänster från leverantörerna.

De deltagare som är upphandlande myndigheter kan komma att behöva genomföra en upphandling för att anskaffa tjänster som tillhandahålls av exempelvis accesspunktsoperatörer eller andra tredjepartsleverantörer som är anslutna till SDK. Ett godkännande att ansluta sig till SDK innebär alltså inte att upphandlingslagstiftningen inte därefter behöver tillämpas. En upphandlande myndighet som vill anlita en accesspunktsoperatör för att koppla upp sig mot infrastrukturen kan således komma att behöva genomföra en offentlig upphandling. En separat bedömning av eventuell upphandlingsplikt måste göras utifrån respektive deltagande upphandlande myndighets förutsättningar.

En tänkbar alternativ modell för att tillhandahålla tredjepartstjänster till deltagarna inom ramen för SDK skulle kunna vara att en tillhandahållande myndighet, exempelvis DIGG, inrättar ett auktorisationssystem för offentliga aktörers räkning, godkänner tredjepartsleverantörer och ingår avtal om aktuella tjänster med leverantörerna. De deltagare som är offentliga aktörer ges därefter tillgång till de aktuella tjänsterna i sin verksamhet genom avtal med den tillhandahållande myndigheten. I samband med offentliga utredningar på närliggande områden har gjorts bedömningen att offentliga aktörers relation till den tillhandahållande

myndigheten och leverantörerna inte aktualiserar någon upphandlingsplikt eftersom det utgör en del av auktorisationssystemet.

Härutöver kan vidare noteras att DIGG kan komma att behöva göra upphandlingspliktiga anskaffningar från olika leverantörer för att kunna driva och förvalta infrastrukturen.

Följande upphandlingsrättsliga förutsättningar kan noteras i förhållande till anslutning av accesspunktsoperatörer och andra tredjepartsleverantörer:

- Godkännande och anslutning av accesspunktsoperatörer och andra tredjepartsleverantörer i förhållande till SDK är sannolikt inte upphandlingspliktigt, förutsatt att det inte rör sig om ett selektivt förfarande på så sätt att DIGG väljer ut endast en eller vissa leverantörer att ingå avtal med avseende leverans av tjänster (mot ersättning) inom ramen för SDK.
- Deltagare behöver sannolikt upphandla anskaffningen av tjänster från accesspunktsoperatörer eller tredjepartsleverantörer. En lösning där ett auktorisationssystem som administreras av DIGG, i egenskap av tillhandahållande myndighet, skulle kunna övervägas och utredas vidare.

4.4.3 Ev. underleverantörers roller

En fråga som kan aktualisera särskilda upphandlingsrättsliga överväganden är hur infrastrukturen kommer att vara organiserad och tillhandahållas till deltagarna. Som noterats ovan kommer DIGG att bära det yttersta ansvaret för tillhandahållande av SDK. Det finns dock möjligheter för DIGG att delegera ansvaret i mindre eller större utsträckning till en eller flera underleverantörer med visst begränsat uppdrag/ansvar.

Om DIGG kommer att vara ensam ansvarig för såväl drift och underhåll som förvaltning av både plattformen och federationen i förhållande till deltagarna aktualiseras inte några särskilda upphandlingsrättsliga frågeställningar beträffande relationen mellan federationsägaren och eventuell underleverantör (eftersom båda rollerna innehas av samma aktör). De upphandlingsrättsliga förutsättningarna i relationen till deltagarna har beskrivits ovan.

DIGG skulle dock kunna välja att anlita en eller flera underleverantörer som får uppdrag att ansvara för delar av SDK genom att driva och underhålla federationen i viss utsträckning. Ett uppdrag som underleverantör förväntas regleras i form av ett samarbets- eller uppdragsavtal som innehåller ömsesidiga förpliktelser och övriga villkor som reglerar vad samarbetet eller uppdraget omfattar och hur det ska utföras.

I det fallet kan det inte uteslutas att delar av uppdraget kan komma att omfatta att underleverantören tillhandahåller eller utför tjänster som i och för sig är upphandlingspliktiga, antingen direkt till DIGG eller till deltagarna. I förhållande till DIGG (i egenskap av federationsägare) skulle det kunna röra sig om olika åtaganden förknippade med rollen som underleverantör, exempelvis anslutning av deltagare, teknisk drift och förvaltning av federationen och liknande, men också att, som underleverantör, tillhandahålla plattformstjänster till deltagarna. I förhållande till deltagarna skulle det kunna vara fråga om att tillhandahålla exempelvis adressboken (eller på annat sätt hantera de adressuppgifter som är nödvändiga för överföring av meddelanden inom ramen för SDK), testklienter och testbäddar (det vill säga, verktyg och miljö för tester), tjänster i samband med anslutningsprocessen, driftsupport och liknande.

I förhållande till DIGG skulle en sådan underleverantör vara att betrakta som vilken annan leverantör som helst och om uppdraget att vara underleverantör innebär att leverantören tillhandahåller eller utför tjänster för DIGGs eller deltagarnas räkning mot ersättning rör det sig sannolikt om tilldelning av ett upphandlingspliktigt kontrakt. Underleverantören kan komma att få ersättning antingen direkt från DIGG eller genom en rätt att ta betalt från deltagarna i ett tjänstekoncessionsupplägg. Eftersom det inte lär finnas ett ägar- eller kontrollförhållande mellan DIGG och underleverantören är det inte möjligt att undgå upphandlingskyldighet med tillämpning av Teckalundantaget i detta led.

Som framgått ovan är bedömningen att ett upplägg där underleverantören är en osjälvständig underleverantör till DIGG inte medför några särskilda överväganden i fråga om underleverantörens relation till deltagarna. Detta torde gälla även om underleverantören tar betalt av deltagarna. Så länge det är DIGG som är federationsägare och avtalspart i förhållande till deltagarna är det DIGG som är att betrakta som eventuell leverantör av upphandlingspliktiga tjänster.

I en situation där underleverantören antingen ges en helt självständig ställning i förhållande till DIGG eller tillhandahåller tjänster direkt till deltagarna (mot ersättning) som inte omfattas av uppdraget att vara underleverantör till DIGG kan upphandlingsskyldighet uppkomma för deltagarna. Som framhållits ovan skulle de deltagarna sannolikt behöva upphandla eventuella anskaffningar från underleverantören beroende på vem aktören är (privat, statlig eller kommunal/regional).

Mot bakgrund av att eventuell underleverantörs ställning i förhållande till DIGG inte är helt definierad uppkommer frågan huruvida en eventuell tilldelning från DIGG till en leverantör av uppdraget som underleverantör kan betraktas som ett tjänstekontrakt enligt LOU eller en tjänstekoncession enligt lagen (2016:1147) om upphandling av koncessioner (LUK).

Frågan om ett uppdrag är att definiera som tjänstekontrakt eller som en tjänstekoncession beror dels på ersättningsformen, dels på vem som bär den så kallade verksamhetsrisken. En tjänstekoncession är i praktiken ett tjänstekontrakt, där ersättning för uppdraget helt eller delvis utgår i form av en rätt att utnyttja föremålet för koncessionen och koncessionshavaren övertar verksamhetsrisken. Med övertagande av verksamhetsrisk avses enligt 1 kap. 22–23 §§ LUK att koncessionshavaren står en efterfrågerisk och/eller utbudsrisk genom att denne i) inte är garanterad att kompenseras för de investeringar som görs och de kostnader som uppstår vid tillhandahållandet av koncessionen och ii) utsätts för en verklig exponering för förändringar på marknaden vid tillhandahållandet av koncessionen. Så kan vara fallet exempelvis om tjänsten inte används i förväntad utsträckning.

Det får förutsättas att eventuell underleverantör skulle ha kostnader för att utföra uppdraget. Förutsatt att underleverantören inte garanteras full täckning av dessa kostnader, samt att underleverantörens kostnadstäckning är beroende av hur många deltagare som ansluter sig till federationen, kommer underleverantören sannolikt anses stå en verksamhetsrisk enligt LUK.

En eventuell tilldelning från DIGG till en leverantör av uppdraget som underleverantör skulle kunna betraktas som en tjänstekoncession enligt LUK som är upphandlingspliktig för det fall leverantören har en självständig ställning som underleverantör och får rätt att ta betalt från deltagarna. Om underleverantören på ett eller annat sätt garanteras full täckning för sina kostnader, exempelvis

genom en garanti eller ovillkorlig ersättning från DIGG eller om underleverantören är att betrakta som en osjälvständig underleverantör till DIGG, är upplägget emellertid inte att betrakta som en koncession, utan får i stället sannolikt betraktas som ett tjänstekontrakt enligt LOU.

Oavsett om avtalsförhållandet mellan DIGG och underleverantören är att betrakta som ett tjänsteavtal eller en tjänstekoncession rör det sig dock om ett upphandlingspliktigt kontrakt, varför avtalet inte kan ingås utan föregående upphandling förutsatt att det inte finns något tillämpligt undantag.

4.4.4 Tillhandahållandet av SDK i samverkan med en offentligrättslig samarbetspartner –Hamburgundantaget

Mot bakgrund av att förhållandet mellan DIGG och eventuell underleverantör sannolikt kommer att omfatta tillhandahållande av upphandlingspliktiga tjänster uppkommer frågan huruvida ett avtal mellan DIGG och en leverantör kan undantas upphandlingsskyldighet enligt det så kallade Hamburgundantaget. Nedan analyseras SDK och parternas förhållande mer utförligt utifrån detta undantag.

Det ska dock redan här noteras att detta undantag endast är tillämpligt om leverantören är en upphandlande myndighet eftersom undantaget endast gäller samarbete mellan upphandlande myndigheter. Det ska även tilläggas att även om ett samarbete mellan DIGG och en leverantör kan komma att undantas upphandlingsplikt med tillämpning av det så kallade Hamburgundantaget, så kan upphandlingsskyldighet ändå uppkomma i ett senare led, när deltagare ska ansluta sig till SDK eller anskaffa tjänster inom ramen för SDK.

Underleverantör kommer i detta avsnitt om Hamburgundantaget fortsättningsvis att benämnas offentligrättslig samarbetspartner eller bara samarbetspartner eftersom det avtalsmässigt rör sig om ett samarbete och inte ett renodlat underleverantörsförhållande.

4.4.4.1 *Samarbete mellan DIGG och en offentligrättslig samarbetspartner för att tillhandahålla en offentlig tjänst i syfte att uppfylla gemensamma mål*

Samarbete mellan upphandlande myndigheter

Utgångspunkten för denna del i analysen är att DIGG kommer att ansvara för plattformen, tillhandahålla plattformstjänster samt inneha rollen som federationsägare medan den offentligrättsliga samarbetsparten kommer att ha rollen som leverantör av en eller flera ansvarsområden. Detta innebär att det avgörande är om själva överenskommelsen mellan DIGG och den offentligrättsliga samarbetspartnern om att fullgöra uppdraget som leverantör bedöms som ett "samarbete". I så fall kan Hamburgundantaget tillämpas – annars inte.

Begreppet "samarbete" har i detta sammanhang inte definierats närmare i vare sig upphandlingslagarna eller bakomliggande direktiv men dess innebörd har till viss del tydliggjorts i rättspraxis. EU-domstolen har konstaterat att det inte kan anses röra sig ett samarbete mellan upphandlande myndigheter när en upphandlande myndighet som ska utföra en uppgift av allmänt intresse väljer att inte helt på egen hand utföra denna uppgift – utan ger en annan, fristående upphandlande myndighet, i uppdrag att utföra ett av de nödvändiga arbetsmomenten mot ersättning. EU-domstolen uttalade bland annat att förberedelsen av ett samarbetsavtal förutsätter att de offentliga organ som avser att ingå ett sådant avtal gemensamt fastställer sina behov och hur dessa ska mötas, till skillnad från ett ordinarie förfarande för offentlig upphandling där behoven i regel bedöms och fastställs ensidigt.³⁸

För att en överenskommelse mellan DIGG och en offentligrättslig samarbetspartner ska kunna utgöra ett så kallat Hamburgsamarbete får överenskommelsen alltså inte vara utformad som ett avtal där DIGG ensidigt definierar behovet av en roll som underleverantör och den offentligrättsliga samarbetsparten åtar sig denna roll för att DIGG ska kunna tillhandahålla SDK enligt DIGGs uppdrag. I sådant fall ligger det närmare till hands att den offentligrättsliga samarbetspartnern betraktas som en vanlig leverantör till DIGG

³⁸ EU-domstolens dom i mål C-429/19, Remondis.

snarare än en samarbetspartner och att uppdraget således inte är att betrakta som ett samarbete.

Det krävs emellertid inte att den offentligrättsliga samarbetspartnern och DIGG har ett lika stort ansvar för utförandet eller att den offentligrättsliga samarbetspartnern måste bidra med samma tjänster som DIGG – så länge båda parter åtar sig att bidra till ett fullgörande av den aktuella tjänsten genom samarbete och att samarbetet omfattar ömsesidiga rättigheter och skyldigheter.

Mot denna bakgrund är bedömningen att det, för att kunna betraktas som ett Hamburgsamarbete enligt ovan, bör krävas en överenskommelse mellan DIGG och den offentligrättsliga samarbetspartnern

- bygger på att den offentligrättsliga samarbetspartnern och DIGG i vart fall i någon grad gemensamt ansvarar gentemot deltagarna för att SDK tillhandahålls, och
- inte begränsar den offentligrättsliga samarbetspartnerns roll till att på uppdrag av DIGG utföra ett nödvändigt arbetsmoment för att DIGG ska kunna tillhandahålla SDK.

Som kommer att utvecklas nedan förutsätts vidare att eventuell ersättning till den offentligrättsliga samarbetspartnern inte går utöver de faktiska kostnaderna för att fullgöra uppdraget som leverantör.

Offentliga tjänster för gemensamma mål

De tjänster som samarbetet ska syfta till att tillhandahålla ska vara "offentliga". Begreppet "*offentliga tjänster*" motsvarar enligt förarbetena till LOU "*allmännyttiga tjänster och uppdrag*".³⁹ Av skäl 33 till LOU-direktivet framgår emellertid att ett samarbete kan omfatta alla typer av verksamhet som sammanhänger med fullgörandet av tjänster och ansvar som förelagts de deltagande myndigheterna eller som de tagit på sig ansvaret för, till exempel. obligatoriska eller frivilliga uppgifter för lokala eller regionala myndigheter eller tjänster som genom lag ålagts vissa organ.

³⁹ Prop. 2015/16:195, s. 966.

Även om skälen till LOU-direktivet alltså öppnar upp för en relativt vid tolkning av begreppet "offentliga tjänster" kan det skönjas en viss restriktivitet i tidig praxis från EU-domstolen, vilket även påtalas i förarbetena till den svenska lagen. En indikation på att en tjänst inte är att anse som en offentlig tjänst kan enligt EU-domstolen exempelvis vara att samarbetet i betydande mån avser tjänster som typiskt sett tillhandhålls av andra aktörer än myndigheter.⁴⁰ Det ska emellertid nämnas att det inte alltid är helt tydligt i EU-domstolens uttalanden om domstolen prövat och underkänt ett undantag från upphandlingsreglerna på grund av att avtalet inte varit tillräckligt präglad av organisationernas samarbete, inte berört offentliga tjänster eller inte varit tillräckligt knutet till allmänintresset.

Offentliga tjänster avser i första hand tjänster för att nå operativa mål i den offentliga verksamheten. Det finns därför visst stöd för att skilja offentliga tjänster från stödverksamhet, det vill säga. sådan verksamhet som inte i sig utgör offentliga tjänster, men som indirekt avser fullgörandet av sådana tjänster (exempelvis administration i form av ekonomitjänster, personal- och lönehanteringssystem, städservice, IT med mera). Upphandlingsmyndigheten har intagit ett restriktivt förhållningssätt och gett uttryck för ståndpunkten att undantaget troligen inte är tillämpligt på ett samarbete mellan två upphandlande myndigheter om samarbetet endast avser stödtjänster.⁴¹ EU-domstolen har dock i ett avgörande fastslagit att även samarbeten kring verksamheter som är underordnade de offentliga tjänsterna kan omfattas om verksamheten bidrar till att tjänsterna kan utföras.⁴²

SDK och de tjänster som SDK omfattar torde kunna klassificeras som stödtjänster med beaktande av att det rör sig om infrastruktur för digital kommunikation. SDK bör kunna jämföras med IT-tjänster och andra liknande tjänster som inte typiskt sett avser utförandet av primära uppgifter i offentlig verksamhet utan snarare är ett stöd till verksamheten i övrigt. I förhållande till i alla fall DIGG blir bedömningen dock mer komplex eftersom den typ av tjänster som det nu rör sig om kan sägas tillhöra kärnan av DIGGs verksamhet då DIGG har i uppdrag att sörja för just digital kommunikation i den offentliga sektorn. För DIGG går det därmed att argumenteras för att SDK och de tjänster som SDK omfattar de facto

⁴⁰ Prop. 2015/16:195 s. 966–967 och där hänvisad EU-praxis.

⁴¹ Upphandlingsmyndighetens rapport 2017:3, *Offentlig avtalssamverkan - om så kallade Hamburgsamarbeten och inköpscentralers möjlighet att bedriva grossistverksamhet*, avsnitt 6.4.5.

⁴² EU-domstolens dom i mål C-796/18, *Informatikgesellschaft für Software-Entwicklung (ISE) mbH mot Stadt Köln och Land Berlin*.

syftar till att DIGG ska nå sina operativa mål. Det bör i vart fall inte ifrågasättas att tjänsterna, om det skulle betraktas som stödtjänster, bidrar till att DIGGs primära verksamhet kan utföras.

Eftersom tjänster, för att utgöra "offentliga tjänster" ska syfta till att uppfylla myndigheternas gemensamma mål krävs även att de offentliga tjänster som genomförs genom samarbetet är gemensamma för samtliga samarbetspartners, det vill säga att samtliga parter kan sägas ha ålagts eller tagit på sig ansvaret för att tillhandahålla aktuella tjänster.

DIGGs övergripande uppdrag är att tillhandahålla förvaltningsgemensamma tjänster och infrastruktur till den offentliga förvaltningen. Uppdraget att utveckla och tillhandahålla SDK är ett specifikt regeringsuppdrag som är kopplat till DIGGs övergripande uppdrag.

Det kan mot bakgrund av ovan argumenteras för att tillhandahållandet av SDK ligger inom ramen för DIGGs offentlighetsrättsliga uppdrag och att det redan av den anledningen ska anses vara en offentlig tjänst.

Med hänsyn till hur begreppet och EU-domstolens praxis har tolkats i svenska rättskällor finns visserligen en risk att SDK ändå inte bedöms vara offentlig eftersom tillhandahållande av säker digital kommunikation till offentliga organ inte anses ligga inom vad som traditionellt avses med begreppet allmännyttiga tjänster och uppdrag. Det kan dock argumenteras för att tillhandahållandet av SDK alltså är en sådan tjänst som visserligen är underordnad offentliga tjänster i form av välfärdstjänster och kommunala tjänster som användarna tillhandahåller men som i så hög grad bidrar till att dessa tjänster genomförs på ett korrekt sätt att undantaget ändå ska kunna tillämpas.

Det är dock osäkert om tillhandahållandet av SDK kan anses syfta till att uppfylla DIGGs och den offentlighetsrättsliga leverantören gemensamma mål. Det skulle vara tydligt att så är fallet om det framgår av myndighetsinstruktion eller i samråd mellan staten och SKR, till exempel genom avtal mellan staten och SKR, att inrättandet av SDK ska vara ett gemensamt uppdrag. Alternativt kan redan nu argumenteras för att det är ett gemensamt mål för hela den offentliga sektorn att säkerställa en väl fungerande digital infrastruktur.

4.4.4.2 *Styrs samarbetet endast av överväganden som hänger samman med allmänintresset*

Som framhållits ovan får Hamburgundantaget inte tillämpas på en överenskommelse som innebär att privata aktörer gynnas. I förarbetena anges att detta innebär att det inte får finnas några privata intressen i de upphandlande organisationer som är parter i kontraktet.

Av skäl 33 i LOU-direktivet framgår att även de ekonomiska överföringarna mellan de deltagande upphandlande myndigheterna ska styras av överväganden som hänger samman med allmänintresset. Upphandlingsmyndigheten har mot den bakgrunden dragit slutsatsen att om någon av parterna i samarbetet gör en vinst genom detsamma verkar även kommersiella intressen styra och att de ekonomiska överföringarna mellan parterna därför bör begränsas till kostnadstäckning.⁴³

Ett samarbete mellan DIGG och den offentligrättsliga samarbetspartnern som går ut på att tillhandahålla SDK till offentliga aktörer och privata aktörer inom offentlig verksamhet bör i sig inte betraktas som annat än styrt av allmänintresset. Detta både med hänsyn till avsaknaden av privata intressen i såväl DIGG som den offentligrättsliga samarbetspartnern och mot bakgrund av den tydliga allmännyttan av resultatet av samarbetet (det vill säga, en fungerande säker digital kommunikation i det offentliga). Under förutsättning att eventuella uppdrag till privata aktörer att tillhandahålla tjänster inom ramen för SDK konkurrensutsätts enligt upphandlingslagstiftningen bör överenskommelsen inte heller leda till att någon privat aktör gynnas.

Med hänsyn till hur skälen till LOU-direktivet har tolkats av bland andra Upphandlingsmyndigheten bör eventuell ekonomisk ersättning till den offentligrättsliga leverantören inom ramen för samarbetet begränsas till kostnadstäckning. Då motsvarande formuleringar återfinns även i skäl 47 i LUK-direktivet är bedömningen att motsvarande överväganden gör sig gällande i ett upplägg där deltagarna utger ersättning direkt till den offentligrättsliga leverantören.

⁴³ Upphandlingsmyndighetens rapport 2017:3, avsnitt 6.4.6.

4.4.4.3 *Kan verksamhetskriteriet uppfyllas*

Ytterligare en förutsättning för att ett samarbete ska kunna omfattas av Hamburgundantaget är att myndigheterna utövar mindre än 20 procent av den verksamhet som berörs av samarbetet på den öppna marknaden.

Av 3 kap. 18 § LOU (respektive 3 kap. 20 § LUK) följer att verksamhetsandelarna ska bestämmas på grundval av respektive upphandlande myndighets eller enhets sammanlagda genomsnittliga omsättning i fråga om varor och tjänster avseende de verksamheter som har omfattats av samarbetet under de tre föregående åren.

Frågan om vad som avses med *”den öppna marknaden”* har inte prövats i praxis. Närmare vägledning ges inte heller i förarbetena till de svenska upphandlingslagarna, i de bakomliggande direktiven eller i skälen till direktiven.

En rent språklig tolkning av begreppet talar för slutsatsen att det är den marknad som är utsatt för konkurrens som avses. Det skulle innebära att den offentlighetsrättsliga samarbetspartnern och DIGG måste utföra mindre än 20 procent av de aktiviteter som tillhandahållandet av SDK innefattar på en konkurrensutsatt marknad. Med hänsyn till att varken DIGG eller den offentlighetsrättsliga samarbetspartnern rimligen kan sägas agera på konkurrensutsatta marknader innebär en sådan tolkning att verksamhetskriteriet uppfylls redan av den anledningen.

En annan tolkning av begreppet, som förespråkas av Upphandlingsmyndigheten och som material från EU-kommissionen ger visst stöd för, är att all verksamhet som sker utanför det aktuella samarbetet utgör verksamhet på den öppna marknaden.⁴⁴ Den praktiska tillämpningen av verksamhetskriteriet blir med en sådan tolkning mycket svår att förutse. Det skulle potentiellt kunna innebära att den offentlighetsrättsliga samarbetspartnern och DIGG, baserat på hur dess verksamhet har sett ut de senaste tre åren, måste ha utfört mindre än 20 procent av de aktiviteter som samarbetet innefattar (det vill säga tillhandahållandet av SDK) till andra aktörer än de som ingår i samarbetet för att undantaget ska kunna tillämpas.

⁴⁴ Upphandlingsmyndighetens rapport 2017:3, s. 73 med hänvisningar till EU-kommissionen i fotnot 185.

Eftersom det saknas vägledande praxis och klagörande uttalanden i doktrin är det mycket svårt att med säkerhet uttala sig om hur verksamhetskriteriet skulle bedömas i förhållande till ett samarbete mellan DIGG och den offentligrättsliga samarbetspartnern kring att tillhandahålla SDK. Även om det på goda grunder kan argumenteras för att verksamhetskriteriet ska anses vara uppfyllt, framför allt med hänsyn till att varken en offentligrättslig samarbetspartner lär bedriva och DIGG inte bedriver verksamhet som i nämnvärd utsträckning är kommersiell till sin karaktär, kan det bara konstateras att det finns en beaktansvärd risk att kriteriet inte skulle anses uppfyllt vid ett samarbete mellan DIGG och den offentligrättsliga samarbetspartnern.

4.4.4.4 Sammanfattande kommentarer avseende ett eventuellt Hamburgsamarbete

Bedömningen av om en överenskommelse mellan DIGG och den offentligrättsliga samarbetspartnern kan anses syfta till att upprätta eller reglera formerna för ett samarbete mellan myndigheterna (som ska säkerställa att de offentliga tjänster som myndigheterna ska utföra tillhandahålls för att uppnå myndigheternas gemensamma mål) förutsätter att den offentligrättsliga samarbetspartnern och DIGG kan sägas samarbeta för att tillhandahålla SDK i dess helhet till de slutliga deltagarna. Samarbetet bör omfatta hela möjligheten till säker digital kommunikation som sådan, snarare än den mer begränsade tjänsten att driva SDK. Utrymmet för att tillämpa Hamburgundantaget minskar för det fall överenskommelsen anses omfatta endast den offentligrättsliga samarbetspartnerns uppdrag som underleverantör eftersom ett sådant uppdrag i större utsträckning riskerar att bedömas som ett renodlat underleverantörsuppdrag snarare än ett samarbete och som en icke-offentlig tjänst.

För att kunna betraktas som ett samarbete bör krävas att överenskommelsen mellan DIGG och den offentligrättsliga samarbetspartnern innebär att

- parterna i vart fall i någon grad gemensamt ansvarar gentemot deltagarna för att SDK tillhandahålls
- inte begränsar den offentligrättsliga samarbetspartens roll till att på uppdrag av DIGG utföra ett nödvändigt arbetsmoment för att DIGG ska kunna tillhandahålla SDK, och

- inte innebär att den offentligrättsliga samarbetsparten får betalt, utöver de faktiska kostnaderna för att fullgöra uppdraget som federationsoperatör.

Det bör uppmärksammas att innebörden av uppdraget som underleverantör behöver definieras noga utifrån slutsatserna ovan för att en överenskommelse mellan DIGG och den offentligrättsliga samarbetsparten ska betraktas som ett samarbete.

Som noterats i inledningen till detta avsnitt ska också framhållas att ett Hamburgsamarbete endast får betydelse i relationen mellan DIGG och den offentligrättsliga samarbetsparten. Eventuell upphandlingskyldighet i andra led eller i förhållande till relationer mellan andra aktörer påverkas inte.