Promemoria

Sekretess och dataskydd i det tekniska systemet enligt EU:s förordning om en gemensam digital ingång (Fi 2023:C)

Promemorians huvudsakliga innehåll

I promemorian behandlas frågor om personuppgiftsbehandling och dataskydd samt offentlighet och sekretess kopplade till det tekniska system för automatiskt utbyte av bevis som regleras i EU:s förordning om en gemensam digital ingång (SDG-förordningen).

Enligt SDG-förordningen ska behöriga myndigheter genom det tekniska systemet göra bevis tillgängliga efter en begäran från en myndighet i en annan medlemsstat. Användningen av det tekniska systemet sker endast efter användarens uttryckliga förfrågan. Vissa av de bevis som ska behandlas kan innehålla uppgifter som omfattas av sekretess. De flesta av dessa bevis rör endast användarna själva och kan lämnas ut med användarnas samtycke. Eftersom SDG-förordningen innehåller en uppgiftsskyldighet för de behöriga myndigheterna kan också sekretessbelagda uppgifter som inte endast rör användarna själva lämnas i det tekniska systemet.

SDG-förordningen utgör rättslig grund för den behandling av personuppgifter som förväntas göras i det tekniska systemet. I genomförandeförordningen till SDG-förordningen finns det tydliga bestämmelser om personuppgiftsansvar och dataskydd. Personuppgiftsbehandlingen i det tekniska systemet bedöms vara förenlig med principerna i EU:s dataskyddsförordning.

I promemorian görs bedömningen att det inte finns behov av författningsändringar i fråga om sekretess och personuppgiftsbehandling för att efterleva kraven i förordningen. Det lämnas dock förslag till författningsändringar för att slå fast att det är Myndigheten för digital förvaltning som ska förvalta det tekniska systemet. Syftet med det är att försäkra att myndigheten har rättsligt stöd för sin personuppgiftsbehandling.

Innehållsförteckning

1 Författningsförslag

1.1 Förslag till förordning om ändring i förordningen (2022:127) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång

Härigenom föreskrivs i fråga om förordningen (2022:127) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång att det ska införas en ny paragraf, 2 a §, med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 a §
	Myndigheten för digital förvaltning är ansvarig för anslutningen till det tekniska systemet för automatiskt bevisutbyte enligt artikel 14 i EU-förordningen.
	Myndigheten ska
	1. ansvara för utveckling, tillgänglighet, underhåll, tillsyn, övervakning och säkerhetshantering av den del av det tekniska systemet som krävs för Sveriges anslutning till det EU-gemensamma tekniska systemet, och
	2. se till att systemet uppfyller de krav som ställs i artikel 14.11 i EU-förordningen och i kommissionens genomförandeförordning (EU) 2022/1463 av den 5 augusti 2022 om fastställande av tekniska och operativa specifikationer för det tekniska systemet för gränsöverskridande automatiskt utbyte av bevis och tillämpning av engångsprincipen i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1724.

Denna förordning träder i kraft den 15 februari 2025.

1.2 Förslag till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning

Härigenom föreskrivs i fråga om förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning att 3 § ska ha följande lydelse.

Lydelse enligt SFS 2024:504	*Föreslagen lydelse*
3 §[1]	
Myndigheten ska	
1. ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift,	
2. främja användningen av elektronisk identifiering och underskrift,	
3. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen, *och*	3. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen,
4. tillhandahålla en förvaltningsgemensam infrastruktur för säker digital kommunikation till verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade.	4. tillhandahålla en förvaltningsgemensam infrastruktur för säker digital kommunikation till verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade, *och*
	5. ansvara för den svenska anslutningen till det tekniska systemet för bevisutbyte i enlighet med Europaparlamentet och rådets förordning (EU) 2018/1724 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 samt rättsakter som

[1] Senaste lydelse 2024:504.

har meddelats med stöd av förordningen.

Denna förordning träder i kraft den 15 februari 2025.

2 Bakgrund

2.1 Ärendet

I juni 2020 färdigställdes promemorian Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen), I 2019:B. I promemorian analyserades och lämnades förslag på hur SDG-förordningen ska kompletteras i svensk rätt. I promemorian gjordes bedömningen att det var för tidigt att bedöma det konkreta lagstiftningsbehovet till följd av de delar av SDG-förordningen som träder i kraft först i december 2023 och att behovet bör utredas på nytt efter det att genomförandeakten avseende det tekniska systemet har beslutats.

Regeringen gav den 13 juni 2023 en utredare uppdrag att utreda och lämna förslag på kompletterande bestämmelser med anledning av den svenska anslutningen till EU:s tekniska system för gränsöverskridande utbyte av bevis. Enligt uppdraget skulle utredaren analysera tre områden: den svenska anslutningen till det tekniska systemet, sekretessfrågor samt frågor om personuppgiftsbehandling (Fi2023/01994). Uppdraget skulle ha redovisats senast den 15 december 2023, men på grund av oförutsedda omständigheter kunde uppdraget aldrig påbörjas.

Regeringen beslutade den 7 mars 2024 att uppdra åt Myndigheten för digital förvaltning att utreda den del av det uppdraget som avser den svenska anslutningen till det tekniska systemet och lämna förslag på vilka åtgärder som behövs med anledning av detta (Fi2024/00654).

Den här promemorian syftar till att utreda de övriga frågorna i uppdraget från den 13 juni 2023, dvs. frågorna om sekretess och personuppgiftsbehandling.

I arbetet med att ta fram promemorian har samråd skett med företrädare för Myndigheten för digital förvaltning, Integritetsskyddsmyndigheten och Skatteverket.

2.2 Allmänt om SDG-förordningen

Den 2 oktober 2018 antog Europaparlamentet och rådet förordning (EU) 2018/1724 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (här kallad SDG-förordningen, efter förkortningen av dess engelska kortnamn, Single Digital Gateway). SDG-förordningen utgör en del av EU:s strategi för den inre marknaden och den fria rörligheten för människor, varor, tjänster och kapital. Med stöd av förordningen ska en gemensam digital ingång inrättas i syfte att minska den administrativa bördan för privatpersoner och företag när de utövar sin rätt till fri rörlighet och utför ärenden eller bedriver verksamhet över gränserna.[1]

[1] Förordningen beskrivs i detalj i den ovan nämnda promemorian från Infrastrukturdepartementet (I 2019:B), Kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång (SDG-förordningen). För en övergripande beskrivning av förordningen och dess syften hänvisas till den promemorian.

En del av den gemensamma digitala ingången utgörs av möjligheten att lämna in bevis online enligt engångsprincipen.[2] Syftet med detta är att privatpersoner och företag inte ska behöva lämna samma data till myndigheter mer än en gång inom EU. Det ska sedan vara möjligt att använda samma data i syfte att utföra gränsöverskridande online-förfaranden som omfattar användare i andra länder (skäl 44 till SDG-förordningen). För att uppnå detta syfte ska kommissionen i samarbete med medlemsstaterna inrätta ett tekniskt system för automatiskt utbyte av bevis mellan behöriga myndigheter i alla medlemsstater (det tekniska systemet). Den del av SDG-förordningen som avser det tekniska systemet ska tillämpas från den 12 december 2023.

[2] På engelska kallas principen the once-only principle. Det tekniska systemet benämns ibland i svenska texter med den engelska förkortningen OOTS – once-only technical system.

3 Det tekniska systemet för automatiskt bevisutbyte

3.1 Regleringen i SDG-förordningen och genomförandeförordningen

Genom SDG-förordningen inrättas en gemensam digital ingång i enlighet med bestämmelserna i förordningen (artikel 2.1). Ingången ska bl.a. ge tillgång till information om förfaranden online och offline och länkar till onlineförfaranden, inbegripet förfaranden som omfattas av bilaga II till förordningen, som inrättats på unionsnivå eller nationell nivå för att användarna ska kunna utöva rättigheterna och efterleva skyldigheterna och reglerna på de områden av den inre marknaden som anges i bilaga I till förordningen (artikel 2.2 b).[3]

Varje medlemsstat ska säkerställa att användare kan få tillgång till och utföra de förfaranden som förtecknas i bilaga II till förordningen helt online, om sådana förfaranden har inrättats i den berörda medlemsstaten (artikel 6.1). Medlemsstaterna ska säkerställa att om ett förfarande som avses i artikel 2.2 b, som inrättats på nationell nivå, kan användas och utföras online av inhemska användare ska det även kunna användas och utföras online av användare i gränsöverskridande situationer på ett icke-diskriminerande sätt genom samma tekniska lösning eller en alternativ teknisk lösning (artikel 13.1).

När det gäller utbyte av bevis för onlineförfaranden som förtecknas i bilaga II till SDG-förordningen och de förfaranden som anges i direktiven 2005/36/EG, 2006/123/EG, 2014/24/EU och 2014/25/EU[4] ska kommissionen i samarbete med medlemsstaterna inrätta ett tekniskt system för automatiskt utbyte av bevis mellan behöriga myndigheter i olika medlemsstater (artikel 14.1).

Om behöriga myndigheter, i sin egen medlemsstat och i elektroniskt format som möjliggör automatiskt utbyte, lagligen utfärdar bevis och som är av relevans för de onlineförfaranden som avses i artikel 14.1 ska de också, för behöriga myndigheter i andra medlemsstater som begär detta, göra sådana bevis tillgängliga i ett elektroniskt format som möjliggör automatiskt utbyte (artikel 14.2).

Det tekniska systemet ska framför allt möjliggöra behandling av begäranden om bevis på användarens uttryckliga förfrågan, möjliggöra behandling av begäranden om åtkomst till eller utbyte av bevis, möjliggöra överföring av bevis mellan behöriga myndigheter, göra det möjligt för den begärande behöriga myndigheten att behandla beviset, säkerställa bevisets

[3] Bilaga I och II täcker ett stort antal rättsområden. I bilaga I nämns bl.a. utbildning och praktik i en annan medlemsstat, hälso- och sjukvård, konsumenträttigheter, gränsöverskridande rättigheter gällande familjer, arbete och pension, fordon m.m. Bilaga II, som är den bilaga som är aktuell för det tekniska systemet för bevisutbyte, redogörs för nedan i avsnitt 4.2.

[4] Direktiv 2005/36/EG om erkännande av yrkeskvalifikationer, direktiv 2006/123/EG om tjänster på den inre marknaden, direktiv 2014/24/EU om offentlig upphandling och om upphävande av direktiv 2004/18/EG samt direktiv 2014/25/EU om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG.

konfidentialitet och integritet, ge användaren möjlighet att förhandsgranska det bevis som ska användas av den begärande myndigheten samt att välja om de ska fortsätta med utbytet av bevis eller inte, säkerställa en tillräcklig nivå av kompatibilitet med andra relevanta system, säkerställa en hög säkerhetsnivå för överföringen och behandlingen av bevis, inte behandla bevis utöver uppgifter som är nödvändiga i tekniskt hänseende för att utbyta beviset, samt behandla bevis endast under den tidsperiod som är nödvändig för detta syfte (artikel 14.3).

Användning av det tekniska systemet ska inte vara obligatorisk för användare och ska endast tillåtas på deras uttryckliga förfrågan, såvida inget annat föreskrivs i unionsrätt eller nationell rätt. Användarna ska tillåtas lämna in bevis på andra sätt än via det tekniska systemet (artikel 14.4).

Ett bevis definieras i SDG-förordningen som dokument eller data, inbegripet text eller ljud, bildinspelningar eller audiovisuella inspelningar, oavsett vilket medium som använts, som en behörig myndighet begär för att bevisa fakta eller överensstämmelse med vissa formkrav i förordningen (artikel 3.5).

En användare är antingen en unionsmedborgare, en fysisk person som bor i en medlemsstat eller en juridisk person som har sitt säte i en medlemsstat, och som använder den information, de förfaranden eller de hjälp- och problemlösningstjänster som avses i artikel 2.2 (artikel 3.1).

En behörig myndighet definieras som en myndighet eller ett organ i en medlemsstat som inrättats på nationell, regional eller lokal nivå och som har specifikt ansvar när det gäller den information, de förfaranden samt de hjälp- och problemlösningstjänster som omfattas av förordningen (artikel 3.4).

Närmare bestämmelser om utformningen av det tekniska systemet finns i kommissionens genomförandeförordning (EU) 2022/1463 om fastställande av tekniska och operativa specifikationer för det tekniska systemet för gränsöverskridande automatiskt utbyte av bevis och tillämpning av engångsprincipen i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1724 (här kallad genomförandeförordningen).

Enligt artikel 4.2 i genomförandeförordningen ska medlemsstaterna säkerställa den tekniska anslutningen mellan de bevisbegärande parternas förfarandeportaler, direkt eller genom förmedlingsplattformar, och de gemensamma tjänsterna samt korrekt registrering av deras datatjänster i de gemensamma tjänsterna. Enligt artikel 4.3 ska medlemsstaterna säkerställa att endast bevisbegärande parter är anslutna, direkt eller genom förmedlingsplattformar, till de gemensamma tjänsterna och att endast bevisbegärande och bevislämnande parter kan använda det tekniska engångssystemet.

Genomförandeförordningen definierar bevislämnande part som en sådan behörig myndighet som avses i artikel 14.2 i SDG-förordningen och som lagligen utfärdar strukturerade eller ostrukturerade bevis (artikel 1.4 i genomförandeförordningen). Bevisbegärande part definieras som behörig myndighet som ansvarar för ett eller flera av eller flera av de förfaranden som avses i artikel 14.1 i SDG-förordningen (artikel 1.5 i genomförandeförordningen).

Medlemsstaterna ska också säkerställa att de bevisbegärande parterna är anslutna till en eIDAS-nod i syfte att möjliggöra användarautentisering

(artikel 3.1). En eIDAS-nod är en förbindelsepunkt för gränsöverskridande elektronisk identifiering som sker med stöd av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen).

3.2 Den tänkta utformningen av systemet i Sverige

Den svenska delen av det tekniska systemet ska tas fram och förvaltas av Myndigheten för digital förvaltning (Digg). Digg utreder för närvarande hur systemet ska utformas och i dagsläget är systemet inte i bruk. I samtal med företrädare för Digg har följande kommit fram om hur systemet är tänkt att utformas.

Den svenska förvaltningsgemensamma infrastrukturen erbjuder i huvudsak två funktioner: en funktion för förmedling och förhandsgranskning vid utlämnande av bevis från svenska myndigheter och en funktion för hämtning och förmedling av bevis från utländska myndigheter till svenska behöriga myndigheter. Funktionen för förmedling av svenska bevis till utländska myndigheter består i huvudsak av följande tre delar:

1. OOTS-noden – en kommunikationskomponent som förmedlar utbytet mellan medlemsländerna.
2. Utrymmet för förhandsgranskning.
3. Datatjänsten, som fungerar som navet i systemet och förmedlar kontakten mellan övriga komponenter i systemet. Den utför också grundläggande funktioner såsom kontroll av datamängder och koppling till auktorisationstjänster och EU-gemensamma tjänster.

OOTS-noden och datatjänsten ingår även i funktionen för hämtning av bevis till Sverige, tillsammans med en särskild komponent för bevishämtning.

Utöver dessa grundkomponenter består systemet av ytterligare delar hos Digg såsom en loggserver och en auktorisationstjänst. Systemet ska också ansluta till dels andra tjänster som Digg tillhandahåller – internationell elektronisk identifiering (eIDAS-nod) och digital post – dels externa tjänster som EU-kommissionen tagit fram, såsom bevismäklare och det semantiska registret. De externa tjänsterna syftar bl.a. till att identifiera vilken benämning och vilka metadata olika bevis kan ha i olika länder.

Systemet har alltså många beståndsdelar och kan uppfattas som komplicerat. Nedan följer en något förenklad beskrivning av hur systemet kommer att fungera i praktiken.

När en användare inleder ett förfarande – t.ex. lämnar in en ansökan – hos en myndighet i en annan medlemsstat och det krävs ett bevis, ska myndigheten på begäran av användaren skicka en förfrågan genom det tekniska systemet om att få ta del av beviset. Om det finns ett bevis som matchar förfrågan skickar det tekniska systemet förfrågan vidare till rätt myndighet i Sverige. Den myndighet som har beviset ska därefter lämna in det till det tekniska systemet. Användaren får sedan möjlighet att förhandsgranska beviset på förmedlingsplattformen. Om användaren godkänner det överlämnas beviset till den begärande myndigheten. Det krävs

att användaren identifierar sig två gånger – först i myndighetens förfarande och sedan innan beviset visas upp för förhandsgranskning.

Under processen skapas olika handlingar: när användaren identifierar sig skapas ett identitetsintyg, och när detta har verifierats mot bevisförfrågan skapas ett åtkomstintyg som skickas till den bevisproducerande myndigheten.

Inget av stegen i processen hanteras manuellt av Diggs personal, utan allt sker automatiskt.

4 Sekretess

4.1 Allmänt

Enligt offentlighetsprincipen har allmänheten rätt att få insyn i statens och kommunens verksamhet, bl.a. genom rätten att ta del av uppgifter som finns i allmänna handlingar hos myndigheter (2 kap. 1 § tryckfrihetsförordningen). Begränsningar av rätten att ta del av allmänna handlingar regleras främst i offentlighets- och sekretesslagen (2009:400), OSL. Sekretess innebär ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL). Sekretess gäller både i förhållande till enskilda personer och andra myndigheter (8 kap. 1–2 §§ OSL). Sekretess gäller också i förhållande till utländska myndigheter och mellanfolkliga organisationer, om inte utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § OSL).

4.2 Handlingar i det tekniska systemet

Det tekniska systemet ska behandla automatiskt utbyte av bevis för onlineförfaranden enligt bilaga II till SDG-förordningen och de förfaranden som anges i direktiven 2005/36/EG, 2006/123/EG, 2014/24/EU och 2014/25/EU (artikel 14.1 i SDG-förordningen). I tabellen nedan anges de förfaranden som framgår av bilaga II och det förväntade resultatet med respektive förfarande.

Livshändelser	**Förfaranden**	**Förväntat resultat med förbehåll för den behöriga myndighetens bedömning av ansökan i enlighet med nationell rätt, där så är relevant**
Födelse	Ansöka om bevis om registrering av födelse	Bevis om registrering av födelse eller födelsebevis
Hemvist	Ansöka om bevis för bosättning	Bekräftelse på aktuell folkbokföringsadress
Studera	Ansöka om studiefinansiering för tertiär utbildning, t.ex. studiebidrag och studielån, från ett offentligt organ eller en offentlig institution	Beslut om ansökan om finansiering eller mottagningsbevis

	Lämna in inledande ansökan om antagning till en offentlig inrättning för högre utbildning	Bekräftelse på mottagande av ansökan
	Ansöka om akademiskt erkännande av examensbevis, utbildningsbevis eller andra bevis på fullgjorda studier eller kurser	Beslut om ansökan om erkännande
Arbeta	Ansöka om beslut om fastställande av tillämplig lagstiftning i enlighet med avdelning II i förordning (EG) nr 883/2004	Beslut om tillämplig lagstiftning
	Anmäla ändrade personliga eller yrkesrelaterade förhållanden avseende den person som erhåller sociala trygghetsförmåner, vilka är relevanta för sådana förmåner	Bekräftelse på mottagande av anmälan om ändring
	Ansöka om europeiskt sjukförsäkringskort	Europeiskt sjukförsäkringskort
	Lämna in en inkomstskattedeklaration	Bekräftelse på mottagande av deklarationen
Flytta	Anmäla adressändring	Bekräftelse på avregistrering från den gamla adressen och registrering på den nya adressen
	Registrera ett motorfordon som ursprungligen kommer från eller redan är registrerat i en medlemsstat, enligt standardförfaranden	Bevis på motorfordonsregistrering

	Erhållande av klistermärken för användning av nationell väg-infrastruktur: tids-baserade avgifter (vinjett), avstånds-baserade avgifter (vägtull), klister-märken för utsläpp utfärdade av ett offentligt organ eller en offentlig institution	Mottagande av vägtulls-märke eller vinjett eller annat bevis på betalning
	Erhållande av klistermärken för utsläpp utfärdade av ett offentligt organ eller en offentlig institution	Mottagande av klister-märke för utsläpp eller annat bevis på betalning
Gå i pension	Ansöka om pension och förmåner vid förtida pensionering från obligatoriska system	Bekräftelse på mot-tagning av ansökan eller beslut om ansökan om pension eller förmåner vid förtida pensionering
	Begära ut inform-ation om uppgifter med anknytning till pension från obligatoriska system	Redovisning av person-liga pensionsuppgifter
Starta företag och bedriva affärsverksamhet	Anmälan av affärs-verksamhet, till-stånd för affärs-verksamhet, ändring av affärs-verksamhet och avslutande av affärsverksamhet utan insolvens- eller likvidationsför-faranden, undan-taget inledande registrering av affärsverksamhet i företagsregistret och undantaget för-faranden för bildande eller senare anmälan av	Bekräftelse på mot-tagande av anmälan eller ändring av – eller av ansökan om tillstånd för – affärsverksamhet

	bolag i den mening som avses i artikel 54 andra stycket i EUF-fördraget	
	Registrera en arbetsgivare (en fysisk person) i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Registrera anställda i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Lämna in en bolagsskattedeklaration	Bekräftelse på mottagande av deklarationen
	Meddela socialförsäkringssystemet när en anställds kontrakt avslutas, dock ej förfaranden för kollektivt avslutande av anställningskontrakt	Bekräftelse på mottagande av meddelandet
	Betala sociala avgifter för anställda	Kvitto eller annan form av bekräftelse på betalningen av sociala avgifter för anställda

Utöver dessa förfaranden ska det tekniska systemet alltså även behandla bevis som utbyts inom ramen för förfaranden enligt Europaparlamentets och rådets direktiv 2005/36/EG av den 7 september 2005 om erkännande av yrkeskvalifikationer (yrkeskvalifikationsdirektivet), Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (tjänstedirektivet) samt Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG och Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (upphandlingsdirektiven).

Det rör sig därmed om ett stort antal olika handlingar på ett antal olika rättsområden. Det kan också tänkas att tillämpningsområdet för artikel 14 kan komma utökas ytterligare i framtiden. Bilaga II har redan utökats genom Europaparlamentets och rådets förordning (EU) 2022/868 av den

30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsförordningen).

4.3 Vissa sekretessbestämmelser av betydelse för det tekniska systemet

Flera av förfarandena i bilaga II involverar handlingar från folkbokföringsregistret. För dessa gäller sekretess för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs (22 kap. 1 § OSL). För förföljda personer gäller sekretess på samma villkor för uppgift om enskilds bostadsadress m.m. som kan användas för att komma i kontakt med denne eller dennes anhöriga, oavsett var uppgiften förekommer (21 kap. 3 § OSL).

Enligt 27 kap. 1 § OSL gäller sekretess i verksamhet som avser bestämmande av skatt eller fastställande av underlag för bestämmande av skatt eller som avser fastighetstaxering för uppgift om en enskilds personliga eller ekonomiska förhållanden. Sekretessen gäller dock inte beslut varigenom skatt eller pensionsgrundande inkomst bestäms eller underlag för bestämmande av skatt fastställs (27 kap. 6 §).

Uppgifter om enskilds hälsotillstånd eller andra personliga förhållanden som förekommer i ärenden enligt lagstiftningen om bl.a. allmän försäkring och allmän pension omfattas av sekretess, om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs (28 kap. 1 § OSL).

Sekretess gäller också i ärende om studiestöd för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde lider skada eller men om uppgiften röjs (28 kap. 9 § OSL).

Vad gäller bevis som utbyts inom ramen för förfaranden enligt upphandlingsdirektiven kan dessa innefatta bl.a. tekniska specifikationer (se artikel 42 i direktiv 2014/24/EU). Enligt 31 kap. 16 § OSL gäller sekretess för uppgift om en enskilds affärs- eller driftförhållanden när denne i vissa fall har trätt i affärsförbindelse med en myndighet, om det av särskild anledning kan antas att den enskilde lider skada om uppgiften röjs. Bestämmelsen har använts för att sekretessbelägga företagshemligheter som har lämnats inom ramen för upphandlingsförfaranden (se t.ex. HFD 2016 ref. 17 och HFD 2017 not. 2).

Det stora flertalet av handlingarna som kommer att utbytas bedöms vara sådana som endast rör en privatperson, t.ex. födelsebevis, universitetsbetyg, bevis om antagning till utbildning, fordonsbevis, utdrag ur bolagsregister och liknande handlingar. Dessa handlingar kommer vanligtvis inte att innehålla uppgifter som omfattas av sekretess, om de inte rör förföljda personer. Vissa uppgifter, t.ex. de som handlar om pension, socialförsäkring och studiestöd, omfattas av sekretessbestämmelser med ett rakt skaderekvisit, vilket innebär att utgångspunkten är att sekretess inte gäller utan att det krävs att den enskilde lider men eller att någon annan form av skada uppstår om uppgifterna skulle röjas. Med hänsyn till de ändamål som bevisen ska uppfylla enligt bilaga II är det inte

troligt att skaderekvisiten kommer att vara uppfyllda, annat än i vissa ovanliga fall.

Handlingar som rör t.ex. upphandling och skatt kan dock mycket väl innehålla sekretessbelagda uppgifter enligt 31 kap. 16 § respektive 27 kap. 1 § OSL. I dessa handlingar kan det också finnas uppgifter som omfattas av sekretess i förhållande till andra personer än den som använder det tekniska systemet.

Här ska också framhållas att det enligt artikel 14.2 endast är sådana bevis som *lagligen utfärdas* av behöriga myndigheter som ska utbytas i det tekniska systemet. Detta kan innebära att inte alla handlingar som hanteras inom ramen för t.ex. ett upphandlingsförfarande behöver göras tillgängliga för utbyte i det tekniska systemet (se vidare i följande avsnitt).

Slutligen ska det poängteras att utbytet av bevis i det tekniska systemet inte innebär en form av direktåtkomst till handlingarna i systemet. Trots att begreppet *automatiskt utbyte av bevis* används i SDG-förordningen rör det sig endast om utbyte på användarens uttryckliga förfrågan (artikel 14.4 och skäl 46).[5] Bestämmelsen om överföring av sekretess vid direktåtkomst enligt 11 kap. 4 § OSL är därför inte aktuell här.

4.4 Behöriga myndigheter

En behörig myndighet enligt SDG-förordningen är en myndighet eller ett organ i en medlemsstat som inrättats på nationell, regional eller lokal nivå och som har specifikt ansvar när det gäller den information, de förfaranden samt de hjälp- och problemlösningstjänster som omfattas av förordningen (artikel 3.4).

Det är upp till varje myndighet och enskilt organ att själva identifiera sig som behörig myndighet enligt definitionen i SDG-förordningen (prop. 2023/24:40).

Digg har tidigare kartlagt vilka som kan vara behöriga myndigheter enligt SDG-förordningen. Kartläggningen indikerade att det finns potentiella behöriga myndigheter i samtliga kommuner och regioner (prop. 2021/22:66 s. 11). Eftersom det tekniska systemet omfattar förfaranden enligt upphandlingsdirektiven framstår detta som en rimlig slutsats.

4.5 Finns det ett behov av ytterligare sekretessbrytande bestämmelser?

Promemorians bedömning: Det saknas behov av att ändra i offentlighets- och sekretesslagen för att uppfylla Sveriges skyldigheter enligt SDG-förordningen eller för att skydda känsliga uppgifter som utbyts i systemet.

[5] Det ska dock nämnas att artikel 14.4 öppnar upp för undantag från detta, om undantaget är föreskrivet i unionsrätt eller nationell rätt.

Skälen för promemorians bedömning

Utgångspunkter

Som framgår i avsnitt 4.3 kan uppgifter hos de behöriga myndigheterna i Sverige i vissa fall omfattas av sekretess. Det innebär att det måste finnas stöd i offentlighets- och sekretesslagen, eller i annan lag eller förordning som den lagen hänvisar till, för att uppgifterna ska kunna lämnas ut till andra myndigheter (jfr 8 kap. 1 § OSL).

De flesta sekretessbestämmelser som nämns i avsnittet – såsom de i 27 kap. 1 §, 28 kap. 1 § och 28 kap. 9 § OSL – gäller endast i specifika verksamheter, dvs. som huvudregel endast hos de myndigheter som handlägger de typer av ärenden där uppgifterna förekommer. Vissa bestämmelser om sekretess gäller dock oavsett var uppgifterna förekommer, t.ex. bestämmelserna i 22 kap. 1 § och 31 kap. 16 § OSL. Det innebär att sekretess enligt dessa bestämmelser även kan gälla hos Digg när handlingarna lämnas i det tekniska systemet.

Sekretess till skydd för en enskild gäller som huvudregel inte i förhållande till den enskilde själv (12 kap. 1 § OSL). I de flesta fall där det tekniska systemet används på begäran av en privatperson för ändamål som bara berör honom eller henne borde eventuell sekretess därför kunna brytas med hjälp av den enskildes samtycke. Som framgår i avsnitt 4.3 kan det dock finnas uppgifter i bevisen som omfattas av sekretess till skydd för annan än den enskilde själv, t.ex. i fråga om förfaranden enligt upphandlingsdirektiven.

Uppgiftsskyldigheten i SDG-förordningen är sekretessbrytande

Enligt 10 kap. 28 § OSL hindrar inte sekretess att en uppgift lämnas ut till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Av 8 kap. 3 § 1 OSL framgår att en uppgift för vilken sekretess gäller inte får röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning.

EU-förordningar bör anses likställda med svensk lag (se t.ex. prop. 1999/2000:126 s. 272). Detta innebär att en uppgiftsskyldighet som följer av en EU-förordning får anses bryta sekretessen enligt 10 kap. 28 § och 8 kap. 3 § OSL (jfr samma prop. s. 283).

I det tekniska systemet kommer uppgiften att lämnas till en annan myndighet genom den plattform som Digg tillhandahåller. Uppgiften kommer sedan att vidareförmedlas till den utländska myndighet som har begärt uppgiften.

Enligt artikel 14.7 i SDG-förordningen finns en skyldighet för de behöriga myndigheterna att genom det tekniska systemet göra bevis tillgängliga efter en begäran från en myndighet i en annan medlemsstat. Detta bedöms utgöra en sådan uppgiftsskyldighet som innebär den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL är tillämplig. Regeringen har tidigare funnit att det i artikel 14 finns en skyldighet för en behörig myndighet att kunna utbyta bevis med en behörig myndighet i en annan medlemsstat (prop. 2021/22:66 s. 13).

Eftersom ett utlämnande genom det tekniska systemet sker i enlighet med särskild föreskrift är också förutsättningarna uppfyllda för att lämna

ut handlingar till en utländsk myndighet enligt 8 kap. 3 § 1 OSL (jfr prop. 2017/18:105 s. 130).

Förhandsgranskningsfunktionen

Det tekniska systemet ska också möjliggöra en förhandsgranskning av det bevis som lämnas ut. Förhandsgranskningen bedöms utgöra ett röjande enligt 3 kap. 1 § OSL. Eftersom det inte rör sig om ett utlämnande till en annan myndighet kan inte den sekretessbrytande bestämmelsen i 10 kap. 28 § tillämpas.

I det här fallet kan i stället handlingarna som huvudregel lämnas ut till den enskilde med stöd av samtycke (se ovan under avsnitt 4.3). Även i de fall då handlingar omfattas av sekretess enligt t.ex. 31 kap. 16 §, dvs. sekretess till skydd för en näringsidkare, så krävs det ju att användaren har rätt att för näringsidkarens räkning inleda ett förfarande där det tekniska systemet används.

Det är alltså sannolikt endast i mycket ovanliga fall som sekretess gäller hos Digg även i förhållande till användaren av förhandsgranskningsfunktionen. Det uppgiftslämnande som kan bli aktuellt bedöms inte vara av den omfattningen att det måste införas en särskild sekretessbrytande bestämmelse för detta ändamål. Om handlingen omfattas av sekretess gentemot användaren får en prövning i stället göras av om ett utlämnande kan ske med stöd av befintliga sekretessbrytande bestämmelser, t.ex. 10 kap. 2 § OSL. Enligt den bestämmelsen hindrar inte sekretess att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.

Uppgifter som inhämtas och skapas genom det tekniska systemet

Det tekniska systemet möjliggör också för svenska myndigheter att hämta in uppgifter från myndigheter i andra EU-länder. Dessa uppgifter inhämtas av samma myndigheter som skulle ha handlagt förfarandet i vanliga fall enligt svenska regler. Samma sekretessbestämmelser som skulle ha varit tillämpliga i ett vanligt nationellt förfarande kommer därför att vara tillämpliga på de bevis som inhämtas av svenska myndigheter från andra medlemsstaters myndigheter med stöd av SDG-förordningen. Det saknas därför behov av ytterligare sekretessbestämmelser för att säkerställa skyddet av särskilt känsliga uppgifter.

Vad gäller de handlingar som skapas hos Digg under användningen av det tekniska systemet – identitetsintyget och åtkomstintyget – bedöms det inte sannolikt att dessa handlingar kommer att innehålla uppgifter som omfattas av sekretess (se avsnitt 3.2). Ett möjligt undantag är uppgifter om förföljda personer, men i den situationen gäller sekretessen oavsett i vilket sammanhang uppgiften förekommer, om övriga kriterier är uppfyllda (21 kap. 3 § OSL).

5 Dataskydd och personuppgiftsbehandling

5.1 Regleringen i SDG-förordningen och genomförandeförordningen

Frågor om dataskydd och personuppgiftsbehandling genomsyrar regleringen av det tekniska systemet. Skäl 42 till SDG-förordningen lyder:

> I syfte att möjliggöra lagligt gränsöverskridande utbyte av bevis och information genom unionsomfattande tillämpning av engångsprincipen, bör denna förordning och engångsprincipen tillämpas i enlighet med alla tillämpliga regler för dataskydd, inbegripet principerna om uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet, nödvändighet, proportionalitet och ändamålsbegränsning. Genomförandet bör också ske i full överensstämmelse med principerna om inbyggd säkerhet och inbyggt integritetsskydd, samt med respekt för enskilda personers grundläggande rättigheter, inbegripet de som avser rättvisa och öppenhet.

I artikel 33 i SDG-förordningen anges att behandlingen av personuppgifter av behöriga myndigheter inom ramen för förordningen ska överensstämma med Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här kallad EU:s dataskyddsförordning. I skäl 43 anges att medlemsstaterna bör säkerställa att användarna ges tydlig information om hur personuppgifter som rör dem kommer att behandlas i enlighet med artiklarna 13 och 14 i EU:s dataskyddsförordning.

Inför antagandet av genomförandeförordningen fördes en diskussion mellan EU-kommissionen och Europeiska datatillsynsmannen om SDG-förordningen ur dataskyddssynpunkt och särskilt om det tekniska systemets förenlighet med EU:s dataskyddsförordning.[6]

I artikel 33 i genomförandeförordningen anges att de behöriga myndigheterna ska agera som personuppgiftsansvariga enligt definitionen i artikel 4.7 i EU:s dataskyddsförordning när det gäller behandling av personuppgifter i bevis som utbyts genom det tekniska systemet och myndigheterna agerar i egenskap av bevisbegärande eller bevislämnande part.

[6] Commission Staff Working Document *Data Protection Impact Assessment accompanying the draft Commission Implementing Act on the technical and operational specifications of the technical system for the crossborder exchange of evidence and application of the OOP,* 2022-08-05, och *Formal comments of the EDPS on the draft Commission Implementing Regulation on the technical and operational specifications of the technical system for the crossborder exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council*, 2021-06-05.

5.2 Personuppgiftsbehandling i det tekniska systemet

EU:s dataskyddsförordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1). Med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller hållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring (artikel 4.2).

Det står klart att såväl bevislämnande som bevisbegärande myndigheter som använder det tekniska systemet kommer att behandla personuppgifter i den mening som avses i EU:s dataskyddsförordning.

Som framgår av avsnitt 4.2 omfattar det tekniska systemet utbyte av en stor mängd olika handlingar och det rör sig därför om en rad olika sorters personuppgifter, även sådana som inte bara rör användaren av systemet.

I de flesta fallen kommer det inte att röra sig om behandling av känsliga personuppgifter enligt artikel 9 i EU:s dataskyddsförordning. Det är dock inte uteslutet att så kan ske, särskilt med beaktande av EU-domstolens praxis på området. I ett avgörande har domstolen funnit att även för- och efternamn på make, sambo eller partner kan utgöra känsliga personuppgifter om dessa indirekt avslöjar uppgifter om sexualliv eller sexuell läggning (EU-domstolens dom i målet OT mot Vyriausioji tarnybinės etikos komisija C-184/20, EU:C:2022:601). Nedan görs därför även en bedömning av om det finns stöd för behandlingen av känsliga personuppgifter.

5.3 Stöd för behandling av personuppgifter

Promemorians bedömning: Det saknas behov av nya bestämmelser med anledning av den personuppgiftsbehandling som kommer att göras av de behöriga myndigheterna till följd av införandet av det tekniska systemet.

För att säkerställa att det finns en rättslig grund för den personuppgiftsbehandling som kommer att göras av Myndigheten för digital förvaltning i sin roll som förvaltare av det tekniska systemet behöver myndighetens roll regleras i författning.

Skälen för promemorians bedömning

Personuppgiftsbehandlingen hos de behöriga myndigheterna

Artikel 5 i EU:s dataskyddsförordning innehåller vissa grundläggande krav som all personuppgiftsbehandling måste uppfylla. Bland dessa kan nämnas att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt. Uppgifterna ska också samlas in för särskilda, uttryckligt angivna

ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (den s.k. finalitetsprincipen).

Vidare krävs att det ska finnas en giltig rättslig grund för varje behandling av personuppgifter. Artikel 6 innehåller en uppräkning av olika typer av rättsliga grunder som personuppgiftsbehandling kan stödja sig på, bl.a. att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c) eller för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e). Enligt artikel 6.3 ska grunden för behandlingen även fastställas i unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

I Sverige kompletteras EU:s dataskyddsförordning bl.a. av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och den tillhörande förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dataskyddslagen är subsidiär i förhållande till andra lagar och förordningar som reglerar hur personuppgifter behandlas, t.ex. myndigheternas registerförfattningar (1 kap. 6 § dataskyddslagen).

Den personuppgiftsbehandling som kommer att ske i det tekniska systemet är nödvändig för att de behöriga myndigheterna ska kunna uppfylla kraven i SDG-förordningen. Som framgår i avsnitt 2.2 är syftet med förordningen att främja den fria rörligheten, vilket måste anses vara ett viktigt allmänt intresse. Personuppgiftsbehandlingen kommer alltså att vara nödvändig för att utföra en uppgift av allmänt intresse och det finns därmed rättslig grund för behandlingen enligt artikel 6.1 e i EU:s dataskyddsförordning.

Som har konstaterats i avsnitt 4.5 utgör bestämmelsen i artikel 14 i SDG-förordningen en uppgiftsskyldighet för de behöriga myndigheterna. Personuppgiftsbehandlingen kommer därför också att vara nödvändig för att fullgöra en rättslig förpliktelse i enlighet med artikel 6.1 c i EU:s dataskyddsförordning.

De behöriga myndigheterna kan också komma att behandla personuppgifter som är känsliga enligt artikel 9.1 i EU:s dataskyddsförordning, t.ex. för att de åtminstone indirekt avslöjar ras eller etniskt ursprung, sexuell läggning eller liknande. Sådana uppgifter är som huvudregel förbjudna att behandla. Undantag från förbudet framgår bl.a. av artikel 9.2 g i EU:s dataskyddsförordning som kompletteras av 3 kap. 3 § dataskyddslagen. Enligt 3 kap. 3 § dataskyddslagen får känsliga personuppgifter behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, t.ex. bestämmelser om hantering av allmänna handlingar. Känsliga personuppgifter får också behandlas om behandlingen är nödvändig för handläggningen av ett ärende. En myndighet får därutöver behandla känsliga personuppgifter om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Enligt 3 kap. 3 § andra stycket dataskyddslagen uppställs dock ett förbud

mot att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Av samma skäl som angetts ovan vad gäller behandlingen av personuppgifter generellt är behandlingen av känsliga personuppgifter nödvändig med hänsyn till det viktiga allmänna intresset av att stärka den fria rörligheten genom att efterleva kraven i SDG-förordningen. Behandlingen är därmed nödvändig med hänsyn till ett viktigt allmänt intresse, förutsatt att behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

I skäl 42 till SDG-förordningen framgår att förordningen ska tillämpas i enlighet med alla tillämpliga regler för dataskydd, inbegripet principerna om uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet, nödvändighet, proportionalitet och ändamålsbegränsning. Genomförandet bör också ske i full överensstämmelse med principerna om inbyggd säkerhet och inbyggt integritetsskydd, samt med respekt för enskilda personers grundläggande rättigheter, inbegripet de som avser rättvisa och öppenhet.

Även genomförandeförordningen innehåller bestämmelser som syftar till att skydda den personliga integriteten. Den bevisbegärande parten eller förmedlingsplattformen ska säkerställa samma skyddsnivå för personuppgifter enligt EU:s dataskyddsförordning som i en situation då användaren överlämnar eller laddar upp beviset utan att använda det tekniska engångssystemet (artikel 34.2). För varje bevisutbyte genom det tekniska systemet ska kontrolleras att det begärda beviset kan matchas med användaren och att användaren har rätt att använda det bevis som begärts (artikel 35.1). Vidare ska funktionen med förhandsgranskning garantera att användarna alltid behåller kontrollen över sina personuppgifter (skäl 23). Slutligen ska systemet innehålla it-säkerhetsgarantier för att förhindra att obehöriga personer får åtkomst (artikel 28 och skäl 28).

Det finns alltså garantier i SDG-förordningen och genomförandeförordningen för att inga obehöriga intrång i den registrerades personliga integritet kommer att ske. Det saknas behov av andra säkerhets- eller skyddsåtgärder i fråga om de behöriga myndigheternas möjlighet att behandla känsliga personuppgifter generellt. I varje enskilt fall är det dock den personuppgiftsansvarige som får bedöma om behandlingen av personuppgifter är förenlig med dataskyddsregleringen.

Slutligen ska tilläggas att vissa av de aktörer som är behöriga myndigheter enligt SDG-förordningen inte är svenska myndigheter – det kan även röra sig om andra organ som har specifikt ansvar när det gäller de förfaranden m.m. som omfattas av SDG-förordningen. För dessa enskilda organ är inte bestämmelsen om undantag mot förbudet att behandla känsliga personuppgifter enligt 3 kap. 3 § dataskyddslagen tillämplig. De känsliga personuppgifter som kommer att behandlas genom SDG-förordningen bedöms endast vara sådana som kommer från förfaranden som Skatteverket, Försäkringskassan och möjligen CSN är ansvariga för. Det är därmed inte troligt att enskilda organ kommer att behandla känsliga personuppgifter inom ramen för SDG-förordningen.

Personuppgiftsbehandlingen hos Digg

Som förvaltare av det tekniska systemet kommer Digg att behandla personuppgifter.

När en bevislämnande part lämnar uppgifter till det systemet kommer Digg att behandla personuppgifter för den bevislämnande partens räkning. Samma sak gäller när bevis hämtas in genom det tekniska systemet för den bevisbegärande partens räkning. Det innebär att Digg kommer att agera som personuppgiftsbiträde i den mening som avses artikel 4.8 i EU:s dataskyddsförordning. Detta framgår även direkt av artikel 35.2 genomförandeförordningen såvitt gäller förhandsgranskningsfunktionen.

När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet (artikel 28.3 i EU:s dataskyddsförordning).

Inom ramen för arbetet med promemorian har det uppkommit frågor om huruvida personuppgiftsbiträdets hantering ska regleras i författning eller genom föreskriftsrätt. Digg kommer dock huvudsakligen att vara personuppgiftsbiträde åt andra myndigheter. Det bedöms därför inte lämpligt att Digg ska utfärda föreskrifter. Vidare rör det sig om en situation där förhållandena i huvudsak ska regleras mellan olika myndigheter. Såvitt är känt finns det inget tidigare exempel i svensk rätt på att villkor för personuppgiftsbiträden fastställs genom författning i en sådan situation. Det bedöms inte heller i det här fallet finnas skäl att reglera villkoren i författning. Regleringen bör i stället ske genom avtal mellan Digg och de myndigheter som lämnar handlingar i det tekniska systemet.

Utöver utbytet av bevis kommer Digg även på egen hand att behandla personuppgifter som personuppgiftsansvarig, framför allt i samband med utfärdandet av åtkomstintyg och identitetsintyg och vid loggningen av uppgifter enligt artikel 17 i genomförandeförordningen. På samma sätt som vid utbytet av bevis i det tekniska systemet får den här personuppgiftsbehandlingen anses vara nödvändig för att uppfylla en rättslig förpliktelse. Det bedöms dock vara nödvändigt att förtydliga att det är just Digg som ska utföra dessa uppgifter för att en rättslig grund ska föreligga. För att det ska finnas en rättslig grund räcker det att det finns föreskrifter på förordningsnivå, t.ex. i förordningen med instruktioner till myndigheten (prop. 2017/18:105 s. 26, 27 och 53). I avsnitt 6 föreslås därför ett sådant förtydligande.

Digg kommer också att behandla personuppgifter i samband med den elektroniska identifieringen av användaren genom en eIDAS-nod. Den här personuppgiftsbehandlingen har diskuterats i tidigare utredningar (se t.ex. avsnitt 7.11 i SOU 2023:61) och det saknas därför skäl att diskutera frågan vidare här.

Särskilt om registerförfattningar

En fråga som har kommit upp i det här arbetet är om det finns bestämmelser i s.k. registerförfattningar – dvs. lagar och förordningar om personuppgiftsbehandlingen hos enskilda myndigheter – som hindrar att personuppgiftsbehandling får ske inom ramen för det tekniska systemet (Se t.ex. promemorian Kompletterande bestämmelser till EU:s förordning

om en gemensam digital ingång [SDG-förordningen], I 2019:B, s. 6 och 7).

En registerförfattning kan avse exempelvis en specifik myndighet eller ett specifikt område. I författningen anges ofta de ändamål för vilka personuppgifterna får behandlas, dvs. lagstiftaren har tagit över uppgiften att bestämma ändamålen och har alltså gjort detta i den personuppgiftsansvariges ställe. Ändamålsregleringen i en registerförfattning kan vara sådan att den uttömmande anger de ändamål för vilka uppgifterna får behandlas. Detta framgår ofta genom att det i författningen anges att personuppgifterna *endast* får behandlas för vissa angivna ändamål. Vidarebehandling för andra ändamål är då inte tillåten (jfr HFD 2021 ref. 10).

Det är vanligt att registerförfattningar innehåller en bestämmelse med innebörden att personuppgifter får behandlas för uppgiftsutlämnande som föreskrivs i lag eller förordning (se t.ex. 114 kap. 9 § socialförsäkringsbalken, 4 § andra stycket studiestödsdatalagen [2009:287] och 6 § andra stycket lagen [2001:454] om behandling av personuppgifter inom socialtjänsten).

Personuppgiftsbehandlingen hos de behöriga myndigheter som lämnar uppgifter i det tekniska systemet har rättsligt stöd i SDG-förordningen. Det bedöms därför i normalfallet saknas behov av att ändra i några befintliga registerförfattningar.

Det finns dock bestämmelser i Skatteverkets registerförfattningar som skulle kunna utgöra ett hinder för Skatteverkets personuppgiftsbehandling enligt SDG-förordningen. Enligt 2 kap. 6 § lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet får uppgifter i Skatteverkets folkbokföringsdatabas lämnas ut till en enskild på medium för automatiserad behandling endast om regeringen har meddelat föreskrifter om det. En motsvarande bestämmelse finns i 2 kap. 6 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

I förarbetena till dessa lagar tycks utländska myndigheter jämställas med enskilda (prop. 2000/01:33 s. 110–113, jfr. SOU 1999:105 s. 256 och 257). När det gäller hanteringen i det tekniska systemet rör det sig i vart fall i slutändan om ett utlämnande till en enskild. Utlämnandet sker på medium för automatiserad behandling. Regeringen har inte meddelat föreskrifter om sådana utlämnanden som sker enligt SDG-förordningen.

De ovan nämnda bestämmelserna i Skatteverkets registerförfattningar bedöms därför stå i strid med skyldigheterna i SDG-förordningen. Eftersom EU-rätten har företräde framför svensk rätt ska dessa bestämmelser och bestämmelser med motsvarande innebörd inte tillämpas på ett sätt som gör att SDG-förordningen inte följs.

Det är givetvis inte en tillfredsställande lösning att en bestämmelse i en lag inte ska tillämpas. Det ska dock nämnas att utredningen Framtidens dataskydd – Vid Skatteverket, Tullverket och Kronofogden (SOU 2023:100) har föreslagit att de nuvarande registerförfattningarna för bl.a. Skatteverket ska upphävas och ersättas av nya författningar. I de föreslagna nya bestämmelserna saknas en motsvarighet till ovan nämnda 2 kap. 6 §. Förslagen bereds för närvarande på Regeringskansliet. Det saknas därför skäl att inom ramen för den här promemorian lämna förslag i frågan.

6 Behov av författningsändringar

Promemorians förslag: I förordningen med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång ska det anges att Myndigheten för digital förvaltning är ansvarig för anslutningen till det tekniska systemet.

Det ska vidare framgå att myndigheten ska

– ansvara för utveckling, tillgänglighet, underhåll, tillsyn, övervakning och säkerhetshantering av den del av det tekniska systemet som krävs för Sveriges anslutning till det EU-gemensamma tekniska systemet,
– se till att systemet uppfyller de krav som ställs på det tekniska systemet i SDG-förordningen och genomförandeförordningen.

Myndighetens roll för ansvar för anslutningen till det tekniska systemet ska även framgå av förordningen med instruktion för Myndigheten för digital förvaltning.

Promemorians bedömning: Det är tillräckligt att regleringen sker i förordning.

Skälen för promemorians förslag och bedömning

Diggs roll behöver författningsregleras

Av 2 § förordningen (2022:127) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång framgår att Digg är nationell samordnare enligt SDG-förordningen. Det framgår dock inte att det är Digg som ska ansvara för förvaltningen och driften av förmedlingsplattformen i det tekniska systemet.

Det framgår förvisso av 1 § tredje stycket förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning att Digg ska ansvara för viss förvaltningsgemensam digital infrastruktur, men det tekniska systemet pekas inte specifikt ut som en del av denna infrastruktur.

Slutligen har Digg i sitt regleringsbrev för 2024 fått i uppdrag ”att vara nationell gemensam kontaktpunkt för tekniskt stöd för att säkerställa drift och underhåll av de relevanta komponenter i det tekniska systemet enligt artikel 21 i [genomförandeförordningen]”. I villkoren för anslagsposten där medel tilldelas framgår att anslagsposten får användas för utveckling och förvaltning av förvaltningsgemensam digital infrastruktur och lösningar som behövs för att möta kraven i SDG-förordningen och genomförandeförordningen samt att anslagsposten även får användas för bidrag till statliga myndigheter, kommuner och regioner, SKR samt Inera AB.

Det saknas alltså ett tydligt utpekande i författning av Digg som ansvarig för systemet. Som framgår i avsnitt 5.3 bedöms detta vara nödvändigt för att det tydligt ska föreligga en rättslig grund för Diggs personuppgiftsbehandling. Det bör därför regleras i författning att Digg ska ansvara för förvaltningen och driften av förmedlingsplattformen i det tekniska systemet.

Ändringarna kan ske genom förordning

En författningsändring som endast påverkar en myndighets arbetsuppgifter kan falla inom regeringens s.k. restkompetens enligt 8 kap. 7 § regeringsformen. Detta gäller så länge inte författningsändringen är en sådan som ska meddelas genom lag enligt 8 kap. 2 § regeringsformen. De föreslagna ändringarna bedöms inte omfattas av någon av situationerna som anges i den bestämmelsen.

Riksdagen har förvisso i lag reglerat frågor om behöriga myndigheter och kontaktpersoner enligt SDG-förordningen. Hanteringen av det tekniska systemet är dock en separat fråga. Frågan har inte heller berörts inom ramen för det tidigare lagstiftningsarbete som har lett till lagen (2022:126) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång och till ändringen av denna (prop. 2021/22:66 och prop. 2023/24:40).

Regleringen av Diggs roll kan därför ske genom en ändring av förordningen med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång.

Enligt artikel 14.11 i SDG-förordningen ska kommissionen och var och en av medlemsstaterna ansvara för utveckling, tillgänglighet, underhåll, tillsyn, övervakning och säkerhetshantering av sina respektive delar av det tekniska systemet. Den föreslagna ändringen i förordningen med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång är baserad på denna formulering. Det föreslås också att det stadgas att det är Digg som ansvarar för att systemet uppfyller de krav som ställs på det tekniska systemet i SDG-förordningen och genomförandeförordningen.

Det tekniska systemet är inte tänkt som ett tidsbegränsat projekt och det bedöms som sannolikt att Digg kommer att driva och förvalta systemet under en längre tid. I syfte att förtydliga myndighetens roll bör därför Diggs ansvar för anslutningen till det tekniska systemet även framgå av förordningen med instruktion för Myndigheten för digital förvaltning. Det finns en liknande formulering av myndighetens roll i genomförandet av eIDAS-förordningen i 3 § 3 myndighetsinstruktionen. Promemorians förslag är baserat på denna formulering.

7 Ikraftträdande- och övergångsbestämmelser

Promemorians förslag: Författningarna ska träda i kraft den 15 februari 2025.

Promemorians bedömning: Inga övergångsbestämmelser behövs.

Skälen för promemorians förslag och bedömning

SDG-förordningen tillämpas i sin helhet från den 12 december 2023. De föreslagna ändringarna tydliggör ansvaret för genomförandet av förordningen och det är därför angeläget att de träder i kraft så snart som möjligt. Den tidigaste tidpunkten för ikraftträdande bedöms vara den 15 februari 2025.

Ändringarna bedöms inte vara sådana att de motiverar särskilda övergångsbestämmelser.

8 Konsekvenser

Förslagen i promemorian kompletterar SDG-förordningen och genomförandeförordningen, som är direkt tillämpliga i Sverige. Konsekvenserna av förordningarna ska inte analyseras här, utan konsekvensanalysen är begränsad till de nationella författningsförslag som lämnas. Förslagen bedöms inte ha några andra effekter än att Diggs ansvar för förvaltningen av det tekniska systemet tydliggörs och att myndigheten får en rättslig grund för viss personuppgiftsbehandling.

Det bedöms inte finnas några alternativa lösningar som är lämpliga för genomförandet av det tekniska systemet i Sverige. De anpassningar som föreslås är nödvändiga för att ge en rättslig grund för Diggs behandling av personuppgifter. Att avstå från att införa nödvändiga bestämmelser utgör alltså inte något alternativ.

Förslagen går inte längre än vad som är nödvändigt för att uppfylla kraven i SDG-förordningen.

Digg har redan tilldelats medel för genomförandet av det tekniska systemet i Sverige och förslagen bedöms inte medföra några kostnader för Digg som inte kan täckas av dessa medel. Förslagen bedöms inte medföra några ytterligare kostnader eller intäkter för staten i övrigt eller för kommuner, regioner, företag och andra enskilda.

Förslagen bedöms överensstämma med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.