KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2022/483

av den 21 mars 2022

om ändring av genomförandebeslut (EU) 2021/1073 om fastställande av tekniska specifikationer och regler för genomförandet av och tillitsramverket för EU:s digitala covidintyg som infördes genom Europaparlamentets och rådets förordning (EU) 2021/953

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2021/953 av den 14 juni 2021 om en ram för utfärdande, kontroll och godtagande av interoperabla intyg om vaccination mot, testning för och tillfrisknande från covid-19 (EU:s digitala covidintyg) för att underlätta fri rörlighet under covid-19-pandemin ([1]), särskilt artikel 9.1, och

av följande skäl:

(1) I förordning (EU) 2021/953 fastställs EU:s digitala covidintyg, som bevisar att en person har fått ett covid-19-vaccin eller ett negativt testresultat eller har tillfrisknat från infektion, för att underlätta innehavarens utövande av sin rätt till fri rörlighet under covid-19-pandemin.

(2) Enligt Europaparlamentets och rådets förordning (EU) 2021/954 ([2]) ska medlemsstaterna tillämpa bestämmelserna i förordning (EU) 2021/953 på tredjelandsmedborgare som inte omfattas av den förordningens tillämpningsområde men som lagligen vistas eller är bosatta på deras territorium och som har rätt att resa till andra medlemsstater i enlighet med unionsrätten.

(3) I rådets rekommendation (EU) 2022/290 om ändring av rådets rekommendation (EU) 2020/912 om de tillfälliga restriktionerna för icke nödvändiga resor till EU och ett eventuellt avskaffande av dessa restriktioner ([3]) föreskrivs att tredjelandsmedborgare som vill göra icke nödvändiga resor från ett tredjeland till unionen bör ha giltiga bevis på vaccination eller tillfrisknande, t.ex. EU:s digitala covidintyg eller ett covid-19-intyg som utfärdats av ett tredjeland som omfattas av en genomförandeakt antagen i enlighet med artikel 8.2 i förordning (EU) 2021/953.

(4) För att EU:s digitala covidintyg skulle kunna användas i hela unionen antog kommissionen genomförandebeslut (EU) 2021/1073 ([4]), för att fastställa tekniska specifikationer och regler för ifyllande, säkert utfärdande och kontroll av EU:s digitala covidintyg och för att säkerställa skyddet av personuppgifter, fastställa den gemensamma strukturen för den unika identifieraren för intyg och utfärda en giltig, säker och interoperabel streckkod.

(5) Enligt artikel 4 i förordning (EU) 2021/953 ska kommissionen och medlemsstaterna inrätta och upprätthålla ett tillitsramverk för EU:s digitala covidintyg. Tillitsramverket kan stödja det bilaterala utbytet av förteckningar över återkallade intyg som innehåller de återkallade intygens unika identifierare för intyg.

([1]) EUT L 211, 15.6.2021, s. 1.

([2]) Europaparlamentets och rådets förordning (EU) 2021/954 av den 14 juni 2021 om en ram för utfärdande, kontroll och godtagande av interoperabla intyg om vaccination mot, testning för och tillfrisknande från covid-19 (EU:s digitala covidintyg) för tredjelandsmedborgare som lagligen vistas eller är bosatta på medlemsstaternas territorier under covid-19-pandemin (EUT L 211, 15.6.2021, s. 24).

([3]) Rådets rekommendation (EU) 2022/290 av den 22 februari 2022 om ändring av rådets rekommendation (EU) 2020/912 om de tillfälliga restriktionerna för icke nödvändiga resor till EU och ett eventuellt avskaffande av dessa restriktioner (EUT L 43, 24.2.2022, s. 79).

([4]) Kommissionens genomförandebeslut (EU) 2021/1073 av den 28 juni 2021 om fastställande av tekniska specifikationer och regler för genomförandet av och tillitsramverket för EU:s digitala covidintyg som infördes genom Europaparlamentets och rådets förordning (EU) 2021/953 (EUT L 230, 30.6.2021, s. 32).

(6) Den 1 juli 2021 driftsattes nätslussen för EU:s digitala covidintyg (*nätslussen*), som är den centrala delen av tillitsramverket och som möjliggör ett säkert och tillförlitligt utbyte mellan medlemsstaterna av öppna nycklar som används för att verifiera EU:s digitala covidintyg.

(7) Tack vare ett framgångsrikt och storskaligt införande har EU:s digitala covidintyg blivit ett mål för bedragare som försöker hitta sätt att utfärda falska intyg. Sådana falska intyg måste därför återkallas. Dessutom kan vissa av EU:s digitala covidintyg återkallas av medlemsstaterna på nationell nivå av medicinska skäl och folkhälsoskäl, till exempel på grund av att en leverans med vacciner som administrerats senare visat sig vara defekt.

(8) EU:s system för digitala covidintyg kan visserligen omedelbart upptäcka förfalskade intyg, men äkta intyg som utfärdats olagligt på grundval av falsk dokumentation, obehörig åtkomst eller med bedrägligt uppsåt kan inte upptäckas i andra medlemsstater såvida inte de förteckningar över återkallade intyg som genereras på nationell nivå blir föremål för utbyte mellan medlemsstaterna. Detsamma gäller för intyg som har återkallats av medicinska skäl och folkhälsoskäl. Om medlemsstaternas kontrollfunktioner inte upptäcker intyg som återkallats av andra medlemsstater utgör detta ett hot mot folkhälsan och undergräver medborgarnas förtroende för EU:s system för digitala covidintyg.

(9) Såsom anges i skäl 19 i förordning (EU) 2021/953 bör medlemsstaterna, av medicinska skäl och folkhälsoskäl och vid förekomst av intyg som utfärdats eller erhållits på olaglig väg samt för de syften som anges i denna förordning, i begränsade fall kunna upprätta och utbyta förteckningar över återkallade intyg, särskilt för intyg som har utfärdats felaktigt, som ett resultat av bedrägeri eller till följd av att en leverans av covid-19-vaccin har visat sig vara defekt. Medlemsstaterna bör inte kunna återkalla intyg som utfärdats av andra medlemsstater. Förteckningar över återkallade intyg som utbyts bör inte innehålla några andra personuppgifter än de unika identifierarna för intyg. De bör framför allt inte ange skälet till att ett intyg har återkallats.

(10) Utöver den allmänna informationen om möjligheten att återkalla intyg och de möjliga skälen till detta bör innehavare av återkallade intyg omgående informeras av den ansvariga utfärdande myndigheten om återkallandet av deras intyg och om skälen till återkallandet. Det kan dock i vissa fall, särskilt när det gäller EU:s digitala covidintyg i pappersform, visa sig vara omöjligt eller innebära en oproportionell ansträngning att spåra och informera innehavaren om återkallandet. Medlemsstaterna bör inte samla in ytterligare personuppgifter som inte behövs för utfärdandeprocessen bara för att kunna informera innehavare av intyg om att deras intyg har återkallats.

(11) Det är därför nödvändigt att stärka tillitsramverket för EU:s digitala covidintyg genom att stödja det bilaterala utbytet av förteckningar över återkallade intyg mellan medlemsstaterna.

(12) Detta beslut omfattar inte tillfälligt upphävande av intyg för nationella användningsfall som inte omfattas av förordningen om EU:s digitala covidintyg, till exempel på grund av att innehavaren av ett vaccinationsintyg har testat positivt för SARS-CoV-2. Det påverkar inte etablerade förfaranden för att kontrollera verksamhetsreglerna för intygens giltighet.

(13) Även om olika strukturer för utbyte av förteckningar över återkallade intyg är möjliga ur teknisk synvinkel är det lämpligast att utbyta dem via nätslussen, eftersom det begränsar datautbytet till det tillitsramverk som redan inrättats och minimerar antalet felpunkter och utbyten mellan medlemsstaterna jämfört med ett alternativt peer-to-peer-system.

(14) I enlighet med detta bör nätslussen för EU:s digitala covidintyg stärkas för att stödja ett säkert utbyte av återkallade digitala covidintyg och säker verifiering av dessa via nätslussen. I detta avseende bör lämpliga säkerhetsåtgärder vidtas för att skydda de personuppgifter som behandlas i nätslussen. För att säkerställa en hög skyddsnivå bör medlemsstaterna pseudonymisera intygens attribut med hjälp av ett oåterkallelig hashvärde som ska föras in i förteckningarna över återkallade intyg. Den unika identifieraren bör betraktas som en pseudonymiserad uppgift för den behandling som utförs inom ramen för nätslussen.

(15) Dessutom bör det fastställas bestämmelser om medlemsstaternas och kommissionens roll när det gäller utbytet av förteckningar över återkallade intyg.

(16) Det är medlemsstaterna eller andra offentliga organisationer eller officiella organ i medlemsstaterna som ansvarar för behandlingen av personuppgifter för innehavare av intyg, och denna behandling bör ske i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ([5]). Behandlingen av personuppgifter inom ramen för kommissionens ansvar att förvalta och säkerställa säkerheten för nätslussen för EU:s digitala covidintyg bör ske i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]).

(17) Medlemsstaterna, företrädda av de utsedda nationella myndigheterna eller offentliga organen, fastställer tillsammans syftet med och metoderna för behandling av personuppgifter genom nätslussen för EU:s digitala covidintyg, och de är därför gemensamt personuppgiftsansvariga. Enligt artikel 26 i förordning (EU) 2016/679 ska gemensamt personuppgiftsansvariga för behandling av personuppgifter under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt den förordningen. Genom artikeln ges också möjlighet att få detta ansvar fastställt genom unionsrätten eller genom medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Det arrangemang som avses i artikel 26 bör införas i bilaga III till detta beslut.

(18) Enligt förordning (EU) 2021/953 ska kommissionen stödja sådana utbyten. Det lämpligaste sättet att fullgöra detta mandat är att sammanställa de inlämnade förteckningarna över återkallade intyg på medlemsstaternas vägnar. Därför bör kommissionen tilldelas rollen som personuppgiftsbiträde för att stödja dessa utbyten genom att underlätta utbytet av förteckningar via nätslussen för EU:s digitala covidintyg på medlemsstaternas vägnar.

(19) Som tillhandahållare av tekniska och organisatoriska lösningar för nätslussen för EU:s digitala covidintyg behandlar kommissionen personuppgifterna i förteckningarna över återkallade intyg i nätslussen på medlemsstaternas vägnar, i deras egenskap av gemensamt personuppgiftsansvariga. Den agerar därför som deras personuppgiftsbiträde. I artikel 28 i förordning (EU) 2016/679 och i artikel 29 i förordning (EU) 2018/1725 fastställs att när uppgifter behandlas av ett personuppgiftsbiträde ska behandlingen regleras genom ett avtal eller en rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och som specificerar behandlingen. Det är därför nödvändigt att fastställa regler för kommissionens behandling av uppgifter i egenskap av personuppgiftsbiträde.

(20) Kommissionens stöduppgift omfattar inte inrättandet av en sådan centraliserad databas som avses i skäl 52 i förordning (EU) 2021/953. Detta förbud syftar till att undvika en centraliserad databas över alla EU:s digitala covidintyg som utfärdats och hindrar inte medlemsstaterna från att utbyta förteckningar över återkallade intyg, vilket uttryckligen föreskrivs i artikel 4.2 i förordning (EU) 2021/953.

(21) När kommissionen behandlar personuppgifter i nätslussen för EU:s digitala covidintyg är den bunden av kommissionens beslut (EU, Euratom) 2017/46 ([7]).

(22) Enligt artikel 3.10 i förordning (EU) 2021/953 får kommissionen anta genomförandeakter som fastställer att covid-19-intyg som utfärdats av ett tredjeland med vilket unionen och medlemsstaterna har ingått ett avtal om fri rörlighet för personer som medger att de avtalsslutande parterna på ett icke-diskriminerande sätt inskränker sådan fri rörlighet av folkhälsoskäl och som inte innehåller någon mekanism för införlivande av unionsrättsakter är likvärdiga med dem som utfärdas i enlighet med denna förordning. På grundval av detta antog kommissionen den 8 juli 2021 genomförandebeslut (EU) 2021/1126 ([8]) om fastställande av likvärdigheten av covid-19-intyg som har utfärdats av Schweiz.

([5]) 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) (EUT L 119, 4.5.2016, s. 1).

([6]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([7]) Kommissionen offentliggör mer information om de säkerhetsstandarder som är tillämpliga på Europeiska kommissionens samtliga informationssystem på https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_sv.

([8]) Kommissionens genomförandebeslut (EU) 2021/1126 av den 8 juli 2021 om fastställande av likvärdigheten av covid-19-intyg som har utfärdats av Schweiz med de intyg som har utfärdats i enlighet med Europaparlamentets och rådets förordning (EU) 2021/953 (EUT L 243, 9.7.2021, s. 49).

(23) Enligt artikel 8.2 i förordning (EU) 2021/953 får kommissionen anta genomförandeakter som fastställer att covid-19-intyg som utfärdats av ett tredjeland i enlighet med standarder och tekniska system som är driftskompatibla med tillitsramverket för EU:s digitala covidintyg och som möjliggör kontroll av intygens äkthet, giltighet och integritet, och som innehåller de uppgifter som anges i bilagan till förordningen ska betraktas som likvärdiga med EU:s digitala covidintyg, i syfte att underlätta innehavarnas utövande av sin rätt till fri rörlighet inom unionen. Såsom anges i skäl 28 i förordning (EU) 2021/953 gäller artikel 8.2 i den förordningen godtagande av intyg som utfärdats av tredjeländer till unionsmedborgare och deras familjemedlemmar. Kommissionen har redan antagit flera sådana genomförandeakter.

(24) För att undvika luckor i upptäckten av återkallade intyg som omfattas av sådana genomförandeakter bör det också vara möjligt för tredjeländer vars covid-19-intyg har bedömts vara likvärdiga i enlighet med artiklarna 3.10 och 8.2 i förordning (EU) 2021/953 att lämna in relevanta förteckningar över återkallade intyg till nätslussen för EU:s digitala covidintyg.

(25) Vissa tredjelandsmedborgare som innehar återkallade covid-19-intyg utfärdade av ett tredjeland vars covid-19-intyg har bedömts vara likvärdiga i enlighet med förordning (EU) 2021/953 kan falla utanför tillämpningsområdet för antingen den förordningen eller förordning (EU) 2021/954 vid den tidpunkt då en förteckning över återkallade intyg som inkluderar deras intyg genereras av det berörda tredjelandet. Vid den tidpunkt då en förteckning över återkallade intyg genereras av ett berört tredjeland går det dock inte att veta om alla tredjelandsmedborgare som innehar återkallade intyg omfattas av tillämpningsområdet för någon av förordningarna. Att försöka utesluta personer som inte omfattas av någon av förordningarna vid den tidpunkt då dessa länders förteckningar över återkallade intyg skapas är därför inte genomförbart, och om man försökte göra detta skulle det leda till att medlemsstaterna inte kan upptäcka återkallade intyg som innehas av tredjelandsmedborgare som reser till unionen för första gången. Även de återkallade intygen för dessa tredjelandsmedborgare skulle dock kontrolleras av medlemsstaterna när deras innehavare reser till unionen, och därefter när de reser inom unionen. De tredjeländer vars intyg har bedömts vara likvärdiga i enlighet med förordning (EU) 2021/953 deltar inte i styrningen av nätslussen och är därför inte gemensamt personuppgiftsansvariga.

(26) Dessutom har EU:s system för digitala covidintyg visat sig vara det enda systemet för covid-19-intyg som fungerar på internationell nivå i stor skala. Till följd av detta har EU:s digitala covidintyg fått allt större global betydelse och bidragit till att hantera pandemin på internationell nivå genom att underlätta säkra internationella resor och global återhämtning. I samband med antagandet av ytterligare genomförandeakter i enlighet med artikel 8.2 i förordning (EU) 2021/953 uppstår nya behov beträffande ifyllandet av EU:s digitala covidintyg. Enligt reglerna i genomförandebeslut (EU) 2021/1073 är efternamn ett obligatoriskt fält i intygets tekniska del. Det är nödvändigt att ändra detta krav för att främja inkludering och driftskompatibilitet med andra system, eftersom det i vissa tredjeländer finns personer utan efternamn. Om namnet på innehavaren av intyget inte kan delas upp i två delar bör namnet placeras i samma fält (efternamn eller förnamn) i EU:s digitala covidintyg, på det sätt som skulle ha gjorts i innehavarens rese- eller identitetshandling. Denna ändring skulle också bättre anpassa det tekniska innehållet i intygen till de nu gällande specifikationerna för maskinläsbara resehandlingar som offentliggjorts av Internationella civila luftfartsorganisationen.

(27) Genomförandebeslut (EU) 2021/1073 bör därför ändras i enlighet med detta.

(28) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 11 mars 2022.

(29) För att ge medlemsstaterna och kommissionen tillräckligt med tid för att genomföra de ändringar som krävs för att möjliggöra utbytet av förteckningar över återkallade intyg via nätslussen för EU:s digitala covidintyg bör detta beslut börja tillämpas fyra veckor efter att det trätt i kraft.

(30) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 14 i förordning (EU) 2021/953.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Genomförandebeslut (EU) 2021/1073 ska ändras på följande sätt:

(1) Följande artiklar ska införas som artiklarna 5a, 5b och 5c:

”*Artikel 5a*

Utbyte av förteckningar över återkallade intyg

1. Tillitsramverket för EU:s digitala covidintyg ska möjliggöra utbyte av förteckningar över återkallade intyg via den centrala nätslussen för EU:s digitala covidintyg (*nätslussen*) i enlighet med de tekniska specifikationerna i bilaga I.

2. När medlemsstaterna återkallar EU:s digitala covidintyg får de lämna in förteckningar över återkallade intyg till nätslussen.

3. När medlemsstaterna lämnar in förteckningar över återkallade intyg ska de utfärdande myndigheterna föra en förteckning över återkallade intyg.

4. När personuppgifter utbyts via nätslussen ska behandlingen begränsas till syftet att stödja utbytet av information om återkallande. Sådana personuppgifter får endast användas för att kontrollera återkallandestatusen för EU:s digitala covidintyg som utfärdats inom ramen för förordning (EU) 2021/953.

5. Den information som lämnas till nätslussen ska omfatta följande uppgifter i enlighet med de tekniska specifikationerna i bilaga I:

a) Pseudonymiserade unika identifierare för intyg för återkallade intyg.

b) Sista giltighetsdatum för den inlämnade förteckningen över återkallade intyg.

6. Om en utfärdande myndighet återkallar EU:s digitala covidintyg som den har utfärdat i enlighet med förordning (EU) 2021/953 eller förordning (EU) 2021/954 och avser att utbyta relevant information via nätslussen ska den överföra den information som avses i punkt 5 i form av förteckningar över återkallade intyg till nätslussen i ett säkert format i enlighet med de tekniska specifikationerna i bilaga I.

7. De utfärdande myndigheterna ska i möjligaste mån tillhandahålla en lösning för att informera innehavarna av återkallade intyg om att deras intyg har återkallats och om skälet till återkallandet vid tidpunkten för återkallandet.

8. Nätslussen ska samla in de förteckningar över återkallade intyg som inkommit. Den ska tillhandahålla verktyg för att skicka ut förteckningarna till medlemsstaterna. Den ska automatiskt radera förteckningarna i enlighet med de sista giltighetsdatum som anges för varje inlämnad förteckning av den myndighet som lämnar in den.

9. De utsedda nationella myndigheter eller officiella organ i medlemsstaterna som behandlar personuppgifter i nätslussen ska vara gemensamt personuppgiftsansvariga för de uppgifter som behandlas. De gemensamt personuppgiftsansvarigas respektive ansvarsområden ska fördelas i enlighet med bilaga VI.

10. Kommissionen ska vara personuppgiftsbiträde för de personuppgifter som behandlas i nätslussen. I egenskap av personuppgiftsbiträde på medlemsstaternas vägnar ska kommissionen säkerställa säkerheten vid överföring och lagring av personuppgifter inom nätslussen och fullgöra personuppgiftsbiträdets skyldigheter enligt bilaga VII.

11. Ändamålsenligheten hos de tekniska och organisatoriska åtgärderna för att säkerställa säkerheten vid behandling av personuppgifter inom nätslussen ska regelbundet testas, bedömas och utvärderas av kommissionen och de gemensamt personuppgiftsansvariga.

Artikel 5b

Tredjeländers inlämning av förteckningar över återkallade intyg

Tredjeländer som utfärdar covid-19-intyg för vilka kommissionen har antagit en genomförandeakt i enlighet med artikel 3.10 eller 8.2 i förordning (EU) 2021/953 får lämna in förteckningar över återkallade covid-19-intyg som omfattas av en sådan genomförandeakt, så att dessa kan behandlas av kommissionen, på de gemensamt personuppgiftsansvarigas vägnar, i den nätsluss som avses i artikel 5a, i enlighet med de tekniska specifikationerna i bilaga I.

Artikel 5c

Styrning av behandlingen av personuppgifter i den centrala nätslussen för EU:s digitala covidintyg

1. Beslutsprocessen för de gemensamt personuppgiftsansvariga ska styras av en arbetsgrupp som inrättats inom ramen för den kommitté som avses i artikel 14 i förordning (EU) 2021/953.

2. De utsedda nationella myndigheter eller officiella organ i medlemsstaterna som behandlar personuppgifter i nätslussen i egenskap av gemensamt personuppgiftsansvariga ska utse företrädare till den gruppen.”

(2) Bilaga I ska ändras i enlighet med bilaga I till det här beslutet.

(3) Bilaga V ska ändras i enlighet med bilaga II till det här beslutet.

(4) Texten i bilaga III till det här beslutet ska läggas till som bilaga VI.

(5) Texten i bilaga IV till det här beslutet ska läggas till som bilaga VII.

Artikel 2

Detta beslut träder i kraft den tredje dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Det ska börja tillämpas fyra veckor efter ikraftträdandet.

Utfärdat i Bryssel den 21 mars 2022.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

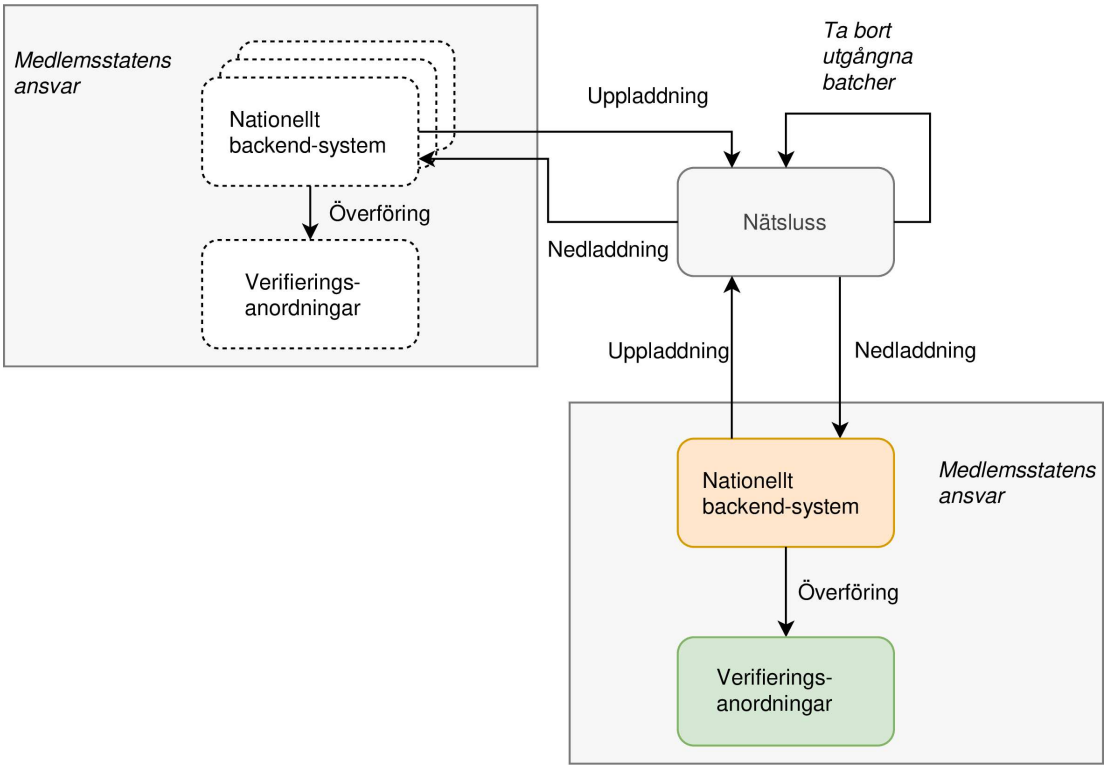
BILAGA I

I bilaga I till genomförandebeslut (EU) 2021/1073 ska följande läggas till som avsnitt 9:

”9. **Systemlösning för återkallande**

9.1 **Tillhandahållande av förteckningar (DRL) över återkallade digitala covidintyg (DCC)**

Nätslussen (gateway) ska ge tillgång till ändpunkter (endpoints) och funktionalitet för att lagra och hantera återkallandeförteckningarna:



9.2 **Tillitsmodell**

Alla anslutningar skapas av den standardiserade tillitsmodellen för nätslussen (DCCG) genom NB_{TLS}- och NB_{UP}-certifikaten (se hantering av certifikat). All information packas och laddas upp med CMS-meddelanden för att säkerställa integriteten.

9.3 **Utformning av batcher**

9.3.1 *Batch*

Varje återkallandeförteckning ska innehålla en eller flera poster och ska packas i batcher som innehåller en uppsättning hashvärden (hashes) och tillhörande metadata. En batch är oföränderlig och har ett utgångsdatum som anger när batchen kan raderas. Alla element i batchen måste ha exakt samma utgångsdatum, vilket innebär att batcherna måste grupperas efter utgångsdatum och efter signerande DSC. Varje batch får innehålla högst 1 000 poster. Om återkallandeförteckningen består av fler än 1 000 poster ska flera batcher skapas. Varje post får förekomma i högst en batch. Batchen ska packas i en CMS-struktur och signeras med det uppladdande landets NB_{up}-certifikat.

9.3.2 *Batchindex*

När en batch skapas ska den tilldelas ett unikt ID av nätslussen och automatiskt läggas till i indexet. Indexet över batcher ordnas efter ändringsdatum, i stigande kronologisk ordning.

9.3.3 *Nätslussens funktion*

Nätslussen behandlar återkallandebatcher utan att göra några ändringar: den kan varken uppdatera, ta bort eller lägga till någon information i batcherna. Batcherna vidarebefordras till alla godkända länder (se kapitel 9.6).

Nätslussen övervakar batchernas utgångsdatum och tar bort utgångna batcher. Efter att batchen har raderats sänder nätslussen tillbaka svaret ”HTTP 410 Gone” för den raderade batchens URL. Batchen anges därför i batchindexet som ”deleted”.

9.4 **Hashtyper**

Återkallandeförteckningen innehåller hashvärden som kan representera olika återkallandetyper/-attribut. Dessa typer eller attribut ska anges vid tillhandahållandet av återkallandeförteckningarna. Följande typer används för närvarande:

Typ	Attribut	Beräkning av hashvärden
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Bara de första 128 bits av hashvärdena, kodade som base64-strängar, läggs in i batcherna och används för att identifiera ett återkallat DCC ([1]).

9.4.1 *Hashtyp: SHA256(DCC-signatur)*

I detta fall beräknas hashvärdet på grundval av samtliga byte för COSE_SIGN1-signaturen från CWT. För RSA-signaturer kommer hela signaturen att användas som indata. Formeln för EC-DSA-signerade certifikat använder r-värdet som indata:

SHA256(r)

[krävs för alla nya tillämpningar]

9.4.2 *Hashtyp: SHA256(UCI)*

I detta fall beräknas hashvärdet på grundval av den UCI-sträng som är kodad i UTF-8 och konverterad till en bytesträng (byte array).

[föråldrad ([2]), men stöds för bakåtkompatibilitet]

9.4.3 *Hashtyp: SHA256(Issuing CountryCode+UCI)*

I detta fall landskod kodad som en UTF-8-sträng, konkatenerad med UCI kodad som en UTF-8-sträng. Detta konverteras sedan till en bytesträng och används som indata till hashfunktionen.

[föråldrad[2], men stöds för bakåtkompatibilitet]

9.5 **API-struktur**

9.5.1 *API för tillhandahållande av återkallandepost*

9.5.1.1 Syfte

API tillhandahåller posterna i återkallandeförteckningen i batcher som inkluderar ett batchindex.

9.5.1.2 Ändpunkter

([1]) Se även de detaljerade API-beskrivningarna i avsnitt 9.5.1.2.

([2]) Föråldrad innebär att denna funktion inte ska användas för nya tillämpningar men ska stödjas för befintliga tillämpningar under en väldefinierad tidsperiod.

9.5.1.2.1 Ändpunkt för nedladdning av batchlista

Ändpunkterna har en enkel utformning och returnerar en batchlista tillsammans med en liten wrapper som innehåller metadata. Batcherna sorteras efter *datum* i *stigande (kronologisk)* ordning:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021–11–01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Anmärkning: Resultatet begränsas automatiskt till 1 000. Om flaggan ”more” är satt till ”true” anger svaret att fler batcher kan laddas ned. För att ladda ned fler element måste klienten sätta headern If-Modified-Since till ett datum som är lika med eller senare än datumet för den senast mottagna posten.

Svaret innehåller en JSON-sträng (array) med följande struktur:

Fält	Definition
more	Boolesk flagga som anger att det finns fler batcher.
batches	Sträng med befintliga batcher.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Landskod enligt ISO 3166.
date	UTC-datum enligt ISO 8601. Datum då batchen lades till eller raderades.
deleted	boolean. ”True” innebär radering. När flaggan för radering är satt kan posten slutligen tas bort från sökresultaten efter 7 dagar.

9.5.1.2.1.1 Svarskoder

Kod	Beskrivning
200	Alla ok.
204	Inget innehåll om headern ”If-Modified-Since” inte har något matchande värde.

Header för begäran

Header	Obligatoriskt	Beskrivning
If-Modified-Since	Ja	Den här headern innehåller datum för senaste nedladdning för att man ska få enbart de senaste resultaten. Vid den första begäran ska headern sättas till ’2021–06–01T00:00:00Z’

9.5.1.2.2 Ändpunkt för nedladdning av batcher

Batcherna innehåller en lista med identifierare för certifikat:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

’country’: ’XY’,

’expires’: ’2022–11–01T00:00:00Z’,

’kid’:‘23S+33f=’,

‘hashType’:‘SIGNATURE’,

’entries’:[{

’hash’:‘e2e2e2e2e2e2e2e2’

}, ..]

}

Svaret innehåller en CMS med en signatur som måste överensstämma med landets NB_{UP}-certifikat. Alla element i JSON-strängen innehåller följande struktur:

Fält	Obligatoriskt	Typ	Definition
expires	Ja	String	Datum då elementet kan tas bort. UTC-datum/tid enligt ISO 8601
country	Ja	String	Landskod enligt ISO 3166.
hashType	Ja	String	Hashtyp för de tillhandahållna posterna (se hashtyper)
entries	Ja	JSON Object Array	Se tabell Poster
kid	Ja	String	base64-kodad KID för det DSC som används för att signera DCC. Om KID är okänd kan strängen `UNKNOWN_KID` (utan`) användas.

Anmärkningar:

— Batcherna ska grupperas efter utgångsdatum och DSC – alla element ska upphöra att gälla samtidigt och ha signerats med samma nyckel.

— Utgångsdatum är ett datum/en tidpunkt i UTC eftersom EU-DCC är ett globalt system och en otvetydig tidsangivelse måste användas.

— Utgångsdatum för ett permanent återkallat DCC ska fastställas till utgångsdatumet för motsvarande DSC som används för att signera DCC eller till den tidpunkt då det återkallade DCC upphör att gälla (Expiration Time; de använda NumericDate/epoch-tiderna ska då betraktas som om de avser UTC-tidszonen).

— Det nationella backend-systemet (NB) ska ta bort element från sin återkallandeförteckning när **utgångsdatumet** infaller.

— *Anm.:* får ta bort element från sin återkallandeförteckning om den **kid** som använts för att signera DCC återkallas.

9.5.1.2.2.1 Poster

Fält	Obligatoriskt	Typ	Definition
hash	Ja	String	De första 128 bits av SHA256-hashen kodade som en base64-sträng

Anmärkning: Objektet ”entries” innehåller för närvarande bara ett hashvärde, men för att säkra kompatibilitet med framtida ändringar valdes ett objekt i stället för en json-sträng.

9.5.1.2.2.2 Svarskoder

Kod	Beskrivning
200	Alla ok.
410	Batchen saknas. Batchen kan raderas i det nationella backend-systemet.

9.5.1.2.2.3 Header för svar

Header	Beskrivning
ETag	Batchens ID

9.5.1.2.3 Ändpunkt för uppladdning av batcher

Uppladdningen görs via samma ändpunkt med verbet POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

’country’: ’XY’,

’expires’: ’2022–11–01T00:00:00Z’,

’kid’:‘23S+33f=’,

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Batchen ska signeras med hjälp av NB_{UP} -certifikatet. Nätslussen ska verifiera att signaturen har angetts med hjälp av NB_{UP} för det berörda landet (*country*). Om signaturen inte godkänns ska uppladdningen inte göras.

ANMÄRKNING: Varje batch är oföränderlig och kan inte ändras efter uppladdning. Den kan dock raderas. ID för varje raderad batch lagras, och en uppladdning av en ny batch med samma ID avvisas.

9.5.1.2.4 Ändpunkt för radering av batcher

En batch kan raderas via samma ändpunkt med verbet DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

eller, av kompatibilitetsskäl, till följande ändpunkt med verbet POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6 **API-skydd – GDPR**

I detta avsnitt anges åtgärder för att tillämpningen ska följa bestämmelserna i förordning (EU) 2021/953 när det gäller behandling av personuppgifter.

9.6.1 *Befintlig autentisering*

Nätslussen använder för närvarande NB_{TLS}-certifikatet för att autentisera de länder som ansluter till nätslussen. Denna autentisering kan användas för att fastställa identiteten för det land som är anslutet till nätslussen. Denna identitet kan sedan användas för att genomföra åtkomstkontroll.

9.6.2 *Åtkomstkontroll*

För att lagligen kunna behandla personuppgifter ska nätslussen använda en mekanism för åtkomstkontroll.

Nätslussen tillämpar en åtkomstkontrollista i kombination med rollbaserad säkerhet (Role Based Security). I det systemet ska två tabeller underhållas – en tabell som beskriver vilka roller (Roles) som kan tillämpa specifika operationer på specifika resurser och en annan tabell som beskriver vilka roller som tilldelas specifika användare (Users).

För att göra de kontroller som krävs enligt detta dokument krävs tre roller, nämligen

RevocationListReader

RevocationUploader

RevocationDeleter

Följande ändpunkter ska kontrollera om användaren har rollen RevocationListReader; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

GET /revocation-list/

GET /revocation-list/{batchId}

Följande ändpunkter ska kontrollera om användaren har rollen RevocationUploader; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

POST /revocation-list

Följande ändpunkter ska kontrollera om användaren har rollen RevocationDeleter; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

DELETE /revocation-list

POST /revocation-list/delete

Nätslussen ska också tillhandahålla en tillförlitlig metod som gör det möjligt för administratörerna att hantera de roller som är kopplade till användarna på ett sådant sätt att risken för mänskliga fel reduceras samtidigt som de funktionella administratörerna inte belastas.”

BILAGA II

Avsnitt 3 i bilaga V till genomförandebeslut (EU) 2021/1073 ska ersättas med följande:

"3. ***Gemensamma strukturer och allmänna krav***

EU:s digitala covidintyg får inte utfärdas om inte alla datafält kan fyllas i korrekt i enlighet med denna specifikation på grund av att information saknas. **Detta ska inte förstås som att det påverkar medlemsstaternas skyldighet att utfärda EU:s digitala covidintyg.**

Informationen i alla fält får tillhandahållas med hjälp av den fullständiga teckenuppsättningen UNICODE 13.0 som kodas med användning av UTF-8, om inte tillhandahållandet är specifikt begränsat till värdeset eller snävare teckenuppsättningar.

Den gemensamma strukturen ska vara följande:

"JSON":{

"ver":<information om version>,

"nam":{

<information om personens namn>

},

"dob":<födelsedatum>,

"v" eller "t" eller "r":[

{<information om vaccinationsdos eller test eller tillfrisknande, en post>}

]

}

Detaljerad information om individuella grupper och fält finns i de följande avsnitten.

Om reglerna anger att ett fält ska hoppas över innebär detta att det ska lämnas tomt och att varken fältets namn eller dess värde får ingå.

3.1. ***Version***

Information om versionen ska tillhandahållas. Versionshanteringen följer Semantic Versioning (semver: https://semver.org). Versionen ska vara en av de versioner som släppts officiellt (nuvarande version eller en av de äldre versioner som släppts officiellt). Se avsnittet JSON-schema – lokalisering för mer detaljer.

Fältets id	Fältets namn	Instruktioner
ver	Schemaversion	Ska motsvara identifieraren för den schemaversion som används för att producera EUDCC. Exempel: "ver":"1.3.0"

3.2. ***Personens namn och födelsedatum***

Personens namn ska vara det fullständiga officiella namnet på personen, som är identiskt med det namn som anges i resehandlingar. Strukturens identifierare är *nam*. Exakt 1 (ett) personnamn ska tillhandahållas.

Fältets id	Fältets namn	Instruktioner
nam/fn	Efternamn (ett eller flera)	Innehavarens efternamn (ett eller flera) Om innehavaren inte har några efternamn men har ett förnamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla efternamn inkluderats. Om det finns flera efternamn ska dessa separeras med mellanslag. Kombinationsnamn där bindestreck eller liknande tecken ingår ska dock vara oförändrade.

		Exempel: ”fn”:”Musterfrau-Gößinger” ”fn”:”Musterfrau-Gößinger Müller”
nam/fnt	Standardiserade efternamn (ett eller flera)	Innehavarens efternamn som translittererats enligt samma konvention som i innehavarens maskinläsbara resehandlingar (såsom de regler som fastställs i Icao Doc 9303 Part 3). Om innehavaren inte har några efternamn men har ett förnamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats, och endast tecknen A-Z och < får användas. Maximal längd: 80 tecken (enligt specifikationen i Icao 9303). Exempel: ”fnt”:”MUSTERFRAU<GOESSINGER” ”fnt”:”MUSTERFRAU<GOESSINGER<MUELLER”
nam/gn	Förnamn (ett eller flera)	Innehavarens förnamn (ett eller flera). Om innehavaren inte har några förnamn men har ett efternamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats. Om det finns flera förnamn ska dessa separeras med mellanslag. Exempel: ”gn”:”Isolde Erika”
nam/gnt	Standardiserade förnamn (ett eller flera)	Innehavarens förnamn som translitterererats enligt samma konvention som i innehavarens maskinläsbara resehandlingar (såsom de regler som fastställs i Icao Doc 9303 Part 3). Om innehavaren inte har några förnamn men har ett efternamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats, och endast tecknen A-Z och < får användas. Maximal längd: 80 tecken. Exempel: ”gnt”:”ISOLDE<ERIKA”
dob	Födelsedatum	DCC-innehavarens födelsedatum. Fullständigt eller partiellt datum men ej tid, begränsat till intervallet 1900-01-01–2099-12-31. Exakt 1 (ett) icke-tomt fält ska tillhandahållas om det fullständiga eller partiella födelsedatumet är känt. Om födelsedatumet inte är känt ens partiellt ska fältet innehålla en tom sträng ””. Detta bör vara identiskt med den information som tillhandahålls i resehandlingar. Ett av följande ISO 8601-format ska användas om information om födelsedatum finns tillgänglig. Andra alternativ stöds inte. YYYY-MM-DD YYYY-MM YYYY (Verifieringsappen kan visa att delar av födelsedatumet saknas med hjälp av den XX-konvention som används i maskinläsbara resehandlingar, t.ex. 1990-XX-XX.) Exempel: ”dob”:”1979-04-14” ”dob”:”1901–08” ”dob”:”1939« ”dob”:””

3.3. ***Grupper för information som är specifik för intygstypen***

JSON-schemat stöder tre grupper av poster som omfattar information som är specifik för intygstypen. Varje EUDCC ska innehålla exakt 1 (en) grupp. Tomma grupper är inte tillåtna.

Gruppidentifierare	**Gruppnamn**	**Poster**
v	Vaccinationsgrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (en) vaccinationsdos (en dos).
t	Testgrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (ett) testresultat.
r	Tillfrisknandegrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (en) utsaga om tillfrisknande. ”

BILAGA III

"BILAGA VI

MEDLEMSSTATERNAS ANSVAR SOM GEMENSAMT PERSONUPPGIFTSANSVARIGA FÖR NÄTSLUSSEN FÖR EU:S DIGITALA COVIDINTYG AVSEENDE UTBYTE AV FÖRTECKNINGAR ÖVER ÅTERKALLANDEN AV EU:S DIGITALA COVIDINTYG

AVSNITT 1

Underavsnitt 1

Ansvarsfördelning

(1) De gemensamt personuppgiftsansvariga ska behandla personuppgifter via tillitsramverkets nätsluss i enlighet med de tekniska specifikationerna i bilaga I.

(2) Medlemsstaternas utfärdande myndigheter förblir den enda personuppgiftsansvariga för insamlingen, användningen, utlämnandet och all annan behandling av uppgifter utanför nätslussen, inbegripet förfarandet som leder till återkallande av ett intyg.

(3) Varje personuppgiftsansvarig ska ansvara för behandlingen av personuppgifter i tillitsramverkets nätsluss i enlighet med artiklarna 5, 24 och 26 i den allmänna dataskyddsförordningen.

(4) Varje personuppgiftsansvarig ska inrätta en kontaktpunkt med en funktionsbrevlåda för kommunikationen mellan de gemensamt personuppgiftsansvariga och mellan de gemensamt personuppgiftsansvariga och personuppgiftsbiträdet.

(5) En arbetsgrupp som inrättas av den kommitté som avses i artikel 14 i förordning (EU) 2021/953 ska ha i uppdrag att fatta beslut i alla frågor som uppstår i samband med utbytet av förteckningar över återkallade intyg och det gemensamma personuppgiftsansvaret för den tillhörande behandlingen av personuppgifter samt för att underlätta samordnade instruktioner till kommissionen i dess egenskap av personuppgiftsbiträde. Beslutsprocessen för de gemensamt personuppgiftsansvariga styrs av arbetsgruppen och den arbetsordning som den ska anta. Grundregeln är att om någon av de gemensamt personuppgiftsansvariga inte deltar i ett arbetsgruppsmöte som har meddelats skriftligen minst sju (7) dagar innan det sammankallas, så innebär detta ett underförstått godkännande av resultatet av detta möte. Vem som helst av de gemensamt personuppgiftsansvariga kan sammankalla ett möte i arbetsgruppen.

(6) Instruktioner till personuppgiftsbiträdet ska skickas via någon av de gemensamt personuppgiftsansvarigas kontaktpunkter, i samförstånd med övriga gemensamt personuppgiftsansvariga och i enlighet med den beslutsprocess för arbetsgruppen som beskrivs i punkt 5 ovan. Den gemensamt personuppgiftsansvariga som tillhandahåller instruktionen bör lämna dem skriftligen till personuppgiftsbiträdet och informera alla andra gemensamt personuppgiftsansvariga om detta. Om den aktuella frågan är så tidskritisk att det inte är möjligt att behandla den vid ett möte i den arbetsgrupp som avses i punkt 5 ovan kan en instruktion ändå ges, men den kan upphävas av arbetsgruppen. Denna instruktion bör ges skriftligen, och alla andra gemensamt personuppgiftsansvariga bör informeras om detta när instruktionen ges.

(7) Den arbetsgrupp som inrättats enligt punkt 5 påverkar inte någon av de gemensamt personuppgiftsansvarigas enskilda befogenhet att informera sin behöriga tillsynsmyndighet i enlighet med artiklarna 33 och 24 i den allmänna dataskyddsförordningen. En sådan anmälan kräver inte samtycke från någon av de andra gemensamt personuppgiftsansvariga.

(8) Inom ramen för tillitsramverkets nätsluss får endast personer som bemyndigats av de utsedda nationella myndigheterna eller officiella organen ha åtkomst till de personuppgifter som utbyts.

(9) Varje utfärdande myndighet ska föra ett register över all behandling som utförts under dess ansvar. Gemensamt personuppgiftsansvar får anges i registret.

Underavsnitt 2

Ansvarsområden och roller vid hantering av begäranden från och information till registrerade

1) Varje personuppgiftsansvarig ska i sin egenskap av utfärdande myndighet förse fysiska personer vars intyg den har återkallat (*de registrerade*) med information om återkallandet och behandlingen av deras personuppgifter i nätslussen för EU:s digitala covidintyg avseende utbytet av förteckningar över återkallande, i enlighet med artikel 14 i den allmänna dataskyddsförordningen, såvida detta inte visar sig vara omöjligt eller skulle innebära en oproportionell ansträngning.

2) Varje personuppgiftsansvarig ska fungera som kontaktpunkt för fysiska personer vars intyg den har återkallat och ska behandla begäranden från de registrerade eller deras företrädare när de utövar sina rättigheter i enlighet med den allmänna dataskyddsförordningen. Om en gemensamt personuppgiftsansvarig tar emot en begäran från en registrerad som avser ett intyg som utfärdats av en annan gemensamt personuppgiftsansvarig ska den informera den registrerade om denna gemensamt personuppgiftsansvarigas identitet och kontaktuppgifter. Om en annan gemensamt personuppgiftsansvarig begär bistånd med hanteringen av registrerades förfrågningar ska de gemensamt personuppgiftsansvariga bistå varandra och svara varandra utan onödigt dröjsmål, senast inom en månad från mottagandet av en begäran om bistånd. Om en begäran avser uppgifter som lämnats in av ett tredjeland ska den personuppgiftsansvariga som tar emot begäran behandla den och informera den registrerade om identitet och kontaktuppgifter för den utfärdande myndigheten i tredjelandet.

3) Varje personuppgiftsansvarig ska ge de registrerade tillgång till innehållet i denna bilaga, inbegripet de arrangemang som fastställs i punkterna 1 och 2.

AVSNITT 2

Hantering av säkerhetsincidenter, inbegripet personuppgiftsincidenter

(1) De gemensamt personuppgiftsansvariga ska bistå varandra i identifiering och hantering av alla säkerhetsincidenter, inbegripet personuppgiftsincidenter, som har koppling till behandlingen i nätslussen för EU:s digitala covidintyg.

2) De gemensamt personuppgiftsansvariga ska särskilt underrätta varandra om följande:

   a) Varje potentiell eller faktisk risk för tillgängligheten till samt sekretessen och/eller integriteten hos de personuppgifter som behandlas i tillitsramverkets nätsluss.

   b) Varje personuppgiftsincident, de sannolika konsekvenserna av personuppgiftsincidenten och bedömningen av risken för fysiska personers rättigheter och friheter samt alla åtgärder som vidtagits för att åtgärda personuppgiftsincidenten och minska risken för fysiska personers rättigheter och friheter.

   c) Varje överträdelse av tekniska och/eller organisatoriska skyddsåtgärder avseende behandlingen i tillitsramverkets nätsluss.

3) De gemensamt personuppgiftsansvariga ska anmäla alla personuppgiftsincidenter som är relaterade till behandlingen i tillitsramverkets nätsluss till kommissionen, till behöriga tillsynsmyndigheter och, när så krävs, till registrerade i enlighet med artiklarna 33 och 34 i den allmänna dataskyddsförordningen eller efter meddelande från kommissionen.

4) Varje utfärdande myndighet ska genomföra lämpliga tekniska och organisatoriska åtgärder för att

   a) säkerställa och skydda tillgängligheten, integriteten och sekretessen hos de personuppgifter som behandlas gemensamt,

   b) skydda mot obehörig eller olaglig behandling, förlust, användning, utlämnande eller förvärv av eller åtkomst till personuppgifter som den innehar,

   c) säkerställa att tillgången till personuppgifterna inte utlämnas till eller tillåts för någon annan än mottagaren eller personuppgiftsbiträdet.

AVSNITT 3

Konsekvensbedömning avseende dataskydd

(1) Om en personuppgiftsansvarig behöver information från en annan personuppgiftsansvarig för att kunna uppfylla sina skyldigheter enligt artiklarna 35 och 36 i förordning (EU) 2016/679 ska en särskild begäran skickas till den funktionsbrevlåda som avses i avsnitt 1 underavsnitt 1.4. Den andra personuppgiftsansvariga ska göra sitt yttersta för att tillhandahålla sådan information.”

BILAGA IV

"BILAGA VII

KOMMISSIONENS ANSVAR SOM PERSONUPPGIFTSBITRÄDE FÖR NÄTSLUSSEN FÖR EU:S DIGITALA COVIDINTYG FÖR ATT STÖDJA UTBYTET AV FÖRTECKNINGAR ÖVER ÅTERKALLANDEN

Kommissionen ska göra följande:

(1) För medlemsstaternas räkning inrätta och säkerställa en säker och tillförlitlig kommunikationsinfrastruktur som stöder utbytet av de förteckningar över återkallanden som lämnas via nätslussen för EU:s digitala covidintyg.

(2) Kommissionen får, för att fullgöra sina skyldigheter som personuppgiftsbiträde för tillitsramverkets nätsluss gentemot medlemsstaterna, anlita tredje parter som underleverantörer. Kommissionen ska informera de gemensamt personuppgiftsansvariga om alla planerade ändringar som rör tillägg av nya eller utbyte av befintliga underleverantörer, och därigenom ge de personuppgiftsansvariga möjlighet att gemensamt invända mot sådana ändringar. Kommissionen ska säkerställa att dataskyddsskyldigheterna i detta beslut även tillämpas på dessa underleverantörer.

(3) Endast behandla personuppgifter på grundval av dokumenterade instruktioner från de personuppgiftsansvariga, såvida inte behandlingen krävs enligt unionsrätten eller en medlemsstats nationella rätt. I sådant fall ska kommissionen informera de gemensamt personuppgiftsansvariga om det rättsliga kravet innan någon behandling av uppgifterna sker, såvida det inte är förbjudet att lämna sådana uppgifter med hänvisning till ett viktigt allmänintresse enligt denna rätt.

Kommissionens behandling omfattar följande:

a) Autentisering av nationella backendservrar, baserat på certifikat för nationella backendservrar.

b) Mottagande av de uppgifter som avses i artikel 5a.3 i beslutet och som laddas upp av nationella backendservrar genom tillhandahållande av ett programmeringsgränssnitt som möjliggör att nationella backendservrar kan ladda upp de relevanta uppgifterna.

c) Lagring av uppgifter i nätslussen för EU:s digitala covidintyg.

d) Tillgängliggörande av uppgifterna för nedladdning av nationella backendservrar.

e) Radering av uppgifterna på deras utgångsdatum eller efter instruktion av den personuppgiftsansvariga som lämnat in dem.

f) När tillhandahållandet av tjänsten har avslutats, radering av alla kvarvarande uppgifter såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

(4) Vidta alla de bästa tillgängliga organisatoriska, fysiska och logiska säkerhetsåtgärder som krävs för att upprätthålla nätslussen för EU:s digitala covidintyg. Kommissionen ska i detta syfte

a) utse en enhet som ansvarar för säkerhetsförvaltningen av nätslussen för EU:s digitala covidintyg, informera de gemensamt personuppgiftsansvariga om enhetens kontaktuppgifter och säkerställa att den kan hantera säkerhetshot,

b) ta ansvaret för säkerheten hos nätslussen för EU:s digitala covidintyg, bland annat genom att regelbundet utföra tester, utvärderingar och bedömningar av säkerhetsåtgärderna,

c) säkerställa att alla personer som beviljas åtkomst till nätslussen för EU:s digitala covidintyg omfattas av avtalsenlig, yrkesmässig eller lagstadgad tystnadsplikt.

(5) Vidta alla nödvändiga säkerhetsåtgärder så att de nationella backendservrarna fungerar smidigt. Kommissionen ska därför införa särskilda förfaranden för anslutning från backendservrarna till nätslussen för EU:s digitala covidintyg. Detta omfattar följande:

a) Ett riskbedömningsförfarande för att identifiera och utvärdera potentiella hot mot systemet.

b) Ett revisions- och granskningsförfarande för att

i. kontrollera sambandet mellan de genomförda säkerhetsåtgärderna och den tillämpliga säkerhetspolicyn,

ii. regelbundet kontrollera systemfilernas, säkerhetsparametrarnas och de beviljade tillståndens integritet,

iii. övervaka att säkerhetsöverträdelser och intrång upptäcks,

iv. genomföra ändringar för att minska befintliga säkerhetsbrister,

v. fastställa villkoren för att tillåta, även på begäran av personuppgiftsansvariga, och bidra till oberoende revisioner, inbegripet inspektioner, och översyner av säkerhetsåtgärder, på villkor som följer protokoll nr 7 till EUF-fördraget om Europeiska unionens immunitet och privilegier.

c) Ändring av kontrollförfarandet för att dokumentera och mäta effekten av en ändring innan den genomförs och hålla de gemensamt personuppgiftsansvariga informerade om samtliga ändringar som kan påverka kommunikationen med och/eller säkerheten i deras infrastrukturer.

d) Inrättande av ett underhålls- och reparationsförfarande för att fastställa de regler och villkor som ska följas vid underhåll och/eller reparation av utrustning.

e) Inrättande av ett förfarande för säkerhetsincidenter för att fastställa ett rapporterings- och eskaleringssystem, information utan dröjsmål till personuppgiftsansvariga som berörs, så att de vid behov även kan informera de nationella dataskyddsmyndigheterna om personuppgiftsincidenter, och fastställande av ett disciplinärt förfarande för att åtgärda dessa.

(6) Vidta bästa tillgängliga fysiska och/eller logiska säkerhetsåtgärder för de anläggningar där utrustningen för nätslussen för EU:s digitala covidintyg finns och för kontroller av åtkomst till logiska data och säkert tillträde. Kommissionen ska i detta syfte göra följande:

a) Införa fysiska säkerhetsåtgärder för att upprätta tydliga säkerhetsperimetrar och möjliggöra att överträdelser upptäcks.

b) Kontrollera tillträdet till anläggningar och upprätthålla ett besöksregister för spårning.

c) Säkerställa att externa personer som beviljas tillträde till lokaler åtföljs av vederbörligen bemyndigad personal.

d) Säkerställa att utrustning inte kan läggas till, ersättas eller avlägsnas utan förhandstillstånd från utsedda ansvariga organ.

e) Kontrollera ömsesidig åtkomst mellan de nationella backendservrarna och tillitsramverkets nätsluss.

f) Säkerställa att personer som får åtkomst till nätslussen för EU:s digitala covidintyg identifieras och autentiseras.

g) Se över de tillståndsrättigheter som gäller åtkomst till nätslussen för EU:s digitala covidintyg vid säkerhetsöverträdelser som påverkar denna infrastruktur.

h) Bevara integriteten hos den information som överförs via nätslussen för EU:s digitala covidintyg.

i) Vidta tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörig åtkomst till personuppgifter.

j) Vid behov vidta åtgärder för att blockera obehörig åtkomst till nätslussen för EU:s digitala covidintyg från de utfärdande myndigheternas domän (dvs. blockera en plats/IP-adress).

(7) Vidta åtgärder för att skydda sin domän, inklusive genom frånkoppling, vid betydande avvikelser från principerna och koncepten för kvalitet eller säkerhet.

(8) Upprätthålla en riskhanteringsplan för sitt ansvarsområde.

(9) Övervaka – i realtid – prestandan för alla tjänstekomponenter i sina tjänster i tillitsramverkets nätsluss, ta fram regelbunden statistik och upprätthålla register.

(10) Ge stöd för alla tjänster i tillitsramverkets nätsluss dygnet runt och året runt på engelska via telefon, e-post eller webbportalen och godta samtal från godkända personer som ringer upp: samordnarna för nätslussen för EU:s digitala covidintyg och deras respektive hjälpcentraler, projektansvariga och utsedda personer från kommissionen.

(11) Bistå de gemensamt personuppgiftsansvariga med lämpliga tekniska och organisatoriska åtgärder, när detta är möjligt i enlighet med artikel 12 i förordning (EU) 2018/1725, i syfte att fullgöra den personuppgiftsansvarigas skyldighet att besvara begäran om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen.

(12) Stödja de gemensamt personuppgiftsansvariga genom att tillhandahålla information om nätslussen för EU:s digitala covidintyg i syfte att fullgöra skyldigheterna enligt artiklarna 32, 33, 34, 35 och 36 i den allmänna dataskyddsförordningen.

(13) Säkerställa att de uppgifter som behandlas i nätslussen för EU:s digitala covidintyg är oläsbara för personer som inte är behöriga att få tillgång till den.

(14) Vidta alla relevanta åtgärder för att förhindra att operatörerna av nätslussen för EU:s digitala covidintyg får obehörig tillgång till överförda uppgifter.

(15) Vidta åtgärder för att underlätta interoperabiliteten och kommunikationen mellan de utsedda personuppgiftsansvariga för nätslussen för EU:s digitala covidintyg.

(16) Föra ett register över behandling som utförts för de gemensamt personuppgiftsansvarigas räkning i enlighet med artikel 31.2 i förordning (EU) 2018/1725.”