KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2022/483

af 21. marts 2022

om ændring af gennemførelsesafgørelse (EU) 2021/1073 om fastsættelse af tekniske specifikationer og regler for gennemførelsen af tillidsrammen for EU's digitale covidcertifikat som fastsat ved Europa-Parlamentets og Rådets forordning (EU) 2021/953

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2021/953 af 14. juni 2021 om en ramme for udstedelse, kontrol og accept af interoperable covid-19-vaccinations-, test- og restitutionscertifikater (EU's digitale covidcertifikat) for at lette fri bevægelighed under covid-19-pandemien ([1]), særlig artikel 9, stk. 1, og

ud fra følgende betragtninger:

(1) I forordning (EU) 2021/953 fastsættes EU's digitale covidcertifikat, der dokumenterer, at en person har modtaget en covid-19-vaccine, har et negativt testresultat eller er kommet sig over sygdommen, med det formål at lette indehaverens mulighed for at udøve sin ret til fri bevægelighed under covid-19-pandemien.

(2) I henhold til Europa-Parlamentets og Rådets forordning (EU) 2021/954 ([2]) skal medlemsstaterne anvende de regler, der er fastsat i forordning (EU) 2021/953, på tredjelandsstatsborgere, der ikke er omfattet af nævnte forordnings anvendelsesområde, men som lovligt opholder sig eller har bopæl på deres område, og som har ret til at rejse til andre medlemsstater i overensstemmelse med EU-retten.

(3) I Rådets henstilling (EU) 2022/290 om ændring af Rådets henstilling (EU) 2020/912 om de midlertidige restriktioner for ikkevæsentlige rejser til EU og eventuel ophævelse af disse restriktioner ([3]) fastsættes det, at tredjelandsstatsborgere, der ønsker at foretage ikkevæsentlige rejser fra et tredjeland til Unionen, bør være i besiddelse af gyldigt bevis for vaccination eller restitution, såsom EU's digitale covidcertifikat eller covid-19-certifikater udstedt af tredjelande, der er omfattet af en gennemførelsesretsakt vedtaget i henhold til artikel 8, stk. 2, i forordning (EU) 2021/953.

(4) For at EU's digitale covidcertifikat kan blive operationelt i hele Unionen, har Kommissionen vedtaget gennemførelsesafgørelse (EU) 2021/1073 ([4]) for at fastsætte de tekniske specifikationer og regler for udfyldelse, sikker udstedelse og kontrol af de digitale covidcertifikater, sikring af beskyttelsen af personoplysninger samt fastsættelsen af den fælles struktur for den unikke certifikatidentifikator og udstedelsen af en gyldig, sikker og interoperabel stregkode.

(5) Kommissionen og medlemsstaterne skulle i henhold til artikel 4 i forordning (EU) 2021/953 oprette og vedligeholde en tillidsramme for EU's digitale covidcertifikat. Denne tillidsramme kan endvidere støtte bilateral udveksling af lister over tilbagekaldte certifikater, der indeholder de unikke certifikatidentifikatorer for tilbagekaldte certifikater.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2021/954 af 14. juni 2021 om en ramme for udstedelse, kontrol og accept af interoperable covid-19-vaccinations-, test- og restitutionscertifikater (EU's digitale covidcertifikat) for så vidt angår tredjelandsstatsborgere, der lovligt opholder sig eller bor på medlemsstaternes område under covid-19-pandemien (EUT L 211 af 15.6.2021, s. 24).

([3]) Rådets henstilling (EU) 2022/290 af 22. februar 2022 om ændring af Rådets henstilling (EU) 2020/912 om de midlertidige restriktioner for ikkevæsentlige rejser til EU og eventuel ophævelse af disse restriktioner (EUT L 43 af 24.2.2022, s. 79).

([4]) Kommissionens gennemførelsesafgørelse (EU) 2021/1073 af 28. juni 2021 om fastsættelse af tekniske specifikationer og regler for gennemførelsen af tillidsrammen for EU's digitale covidcertifikat som fastsat ved Europa-Parlamentets og Rådets forordning (EU) 2021/953 (EUT L 230 af 30.6.2021, s. 32).

(6) Den 1. juli 2021 blev portalen for EU's digitale covidcertifikat (»portalen«), som er den centrale del af tillidsrammen og giver mulighed for sikker og pålidelig udveksling mellem medlemsstaterne af de offentlige nøgler, der anvendes til kontrol af EU's digitale covidcertifikater, taget i brug.

(7) Som følge af den vellykkede og omfattende udrulning af EU's digitale covidcertifikater er certifikaterne blevet et mål for svindlere, der forsøger at finde metoder til at udstede svigagtige certifikater. Disse svigagtige certifikater skal derfor tilbagekaldes. Desuden kan visse af EU's digitale covidcertifikater tilbagekaldes af medlemsstaterne på nationalt plan af medicinske og folkesundhedsmæssige årsager, f.eks. hvis det senere konstateres, at et parti allerede givne vacciner var defekt.

(8) Selv om systemet med EU's digitale covidcertifikater er i stand til straks at afsløre forfalskede certifikater, kan ægte certifikater, der er ulovligt udstedt på grundlag af falsk dokumentation, uautoriseret adgang eller med svigagtig hensigt, ikke opdages i andre medlemsstater, medmindre listerne over tilbagekaldte certifikater, der genereres på nationalt plan, udveksles mellem medlemsstaterne. Det samme gælder for certifikater, der er blevet tilbagekaldt af medicinske og folkesundhedsmæssige årsager. Hvis medlemsstaternes kontrolapplikationer ikke opdager certifikater, der er tilbagekaldt af andre medlemsstater, udgør det en trussel mod folkesundheden og underminerer borgernes tillid til systemet med EU's digitale covidcertifikater.

(9) Som anført i betragtning 19 i forordning (EU) 2021/953 bør medlemsstaterne af medicinske og folkesundhedsmæssige årsager og i tilfælde af certifikater, som er uretmæssigt udstedt eller opnået, med henblik på den nævnte forordning være i stand til at oprette og udveksle lister over tilbagekaldte certifikater med andre medlemsstater i begrænsede tilfælde, navnlig i forbindelse med certifikater, der er udstedt fejlagtigt, som følge af svig eller efter suspension af et covid-19-vaccineparti, der har vist sig at være defekt. Medlemsstaterne bør ikke kunne tilbagekalde certifikater, der er udstedt af andre medlemsstater. De udvekslede lister over tilbagekaldte certifikater bør ikke indeholde andre personoplysninger end de unikke certifikatidentifikatorer. De bør navnlig ikke indeholde en begrundelse for, hvorfor et certifikat er blevet tilbagekaldt.

(10) Ud over de generelle oplysninger om muligheden for tilbagekaldelse af certifikater og de mulige årsager hertil bør indehavere af tilbagekaldte certifikater straks underrettes af den ansvarlige udstedelsesmyndighed om tilbagekaldelsen af deres certifikater og begrundelsen for tilbagekaldelsen. Det kan imidlertid i visse tilfælde, og navnlig for så vidt angår de af EU's digitale covidcertifikater, der udstedes på papir, være umuligt eller indebære en uforholdsmæssig stor indsats at spore og underrette indehaveren om tilbagekaldelsen. Medlemsstaterne bør ikke indsamle yderligere personoplysninger, der ikke er nødvendige for udstedelsesprocessen, blot for at kunne underrette certifikatindehavere, hvis deres certifikater tilbagekaldes.

(11) Det er derfor nødvendigt at styrke tillidsrammen for EU's digitale covidcertifikat ved at støtte den bilaterale udveksling af lister over tilbagekaldte certifikater mellem medlemsstaterne.

(12) Denne afgørelse omfatter ikke midlertidig suspension af certifikater til nationale anvendelsestilfælde uden for anvendelsesområdet for forordningen om EU's digitale covidcertifikat, f.eks. hvis indehaveren af et vaccinationscertifikat er testet positiv for sars-CoV-2. Det berører ikke de fastlagte procedurer for kontrol af de forretningsregler, der gælder for certifikaters gyldighed.

(13) Selv om det ud fra et teknisk synspunkt er muligt at anvende forskellige arkitekturer til udveksling af lister over tilbagekaldte certifikater, er det mest hensigtsmæssigt at udveksle dem via portalen, da dataudvekslingen dermed er begrænset til den tillidsramme, der allerede er etableret, og da det minimerer antallet både af mulige fejlpunkter og af udvekslinger mellem medlemsstaterne sammenlignet med et alternativt peer-to-peer-system.

(14) Portalen for EU's digitale covidcertifikat bør derfor styrkes for at støtte sikker udveksling af tilbagekaldte digitale covidcertifikater og sikker kontrol af dem via portalen. I den forbindelse bør der gennemføres passende sikkerhedsforanstaltninger til beskyttelse af de personoplysninger, der behandles i portalen. For at sikre et højt beskyttelsesniveau bør medlemsstaterne pseudonymisere certifikaternes attributter ved hjælp af en irreversibel hash, der skal medtages i listerne over tilbagekaldte certifikater. Den unikke identifikator bør betragtes som pseudonymiserede oplysninger for de behandlingsaktiviteter, der udføres inden for rammerne af portalen.

(15) Desuden bør der fastsættes bestemmelser om medlemsstaternes og Kommissionens rolle med hensyn til udveksling af lister over tilbagekaldte certifikater.

(16) Behandlingen af certifikatindehaveres personoplysninger, som foretages under ansvar af medlemsstaterne eller andre offentlige organisationer eller officielle organer i medlemsstaterne, bør foretages i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([5]). Behandling af personoplysninger under Kommissionens ansvar med henblik på forvaltning og sikring af sikkerheden i portalen for EU's digitale covidcertifikat bør ske i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]).

(17) Medlemsstaterne, der er repræsenteret ved de udpegede nationale myndigheder eller officielle organer, fastlægger i fællesskab formålet med og midlerne til behandling af personoplysninger via portalen for EU's digitale covidcertifikat og er derfor fælles dataansvarlige. Ved artikel 26 i forordning (EU) 2016/679 pålægges de fælles dataansvarlige for behandling af personoplysninger en forpligtelse til på en gennemsigtig måde at fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til samme forordning. Ved nævnte artikel fastsættes også muligheden for, at disse ansvar kan fastlægges i EU-retten eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt. Den ordning, der er omhandlet i artikel 26, bør opføres i bilag III til denne afgørelse.

(18) I henhold til forordning (EU) 2021/953 har Kommissionen til opgave at støtte sådanne udvekslinger. Den mest hensigtsmæssige måde at opfylde dette mandat på er at samle de indsendte lister over tilbagekaldte certifikater på medlemsstaternes vegne. Kommissionen bør derfor tildeles en rolle som databehandler og dermed støtte disse udvekslinger ved at lette udvekslingen af lister via portalen for EU's digitale covidcertifikat på medlemsstaternes vegne.

(19) Som udbyder af tekniske og organisatoriske løsninger til portalen for EU's digitale covidcertifikat behandler Kommissionen personoplysningerne i listerne over tilbagekaldte certifikater i portalen på vegne af medlemsstaterne som fælles dataansvarlige. Den fungerer derfor som databehandler for dem. I henhold til artikel 28 i forordning (EU) 2016/679 og artikel 29 i forordning (EU) 2018/1725 skal en databehandlers behandling være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og som præciserer, hvad behandlingen omfatter. Det er derfor nødvendigt at fastsætte regler for den behandling, som Kommissionen foretager som databehandler.

(20) Kommissionens støtteopgave indebærer ikke oprettelse af en central database som omhandlet i betragtning 52 i forordning (EU) 2021/953. Dette forbud har til formål at undgå et centralt register over alle EU's udstedte digitale covidcertifikater og forhindrer ikke medlemsstaterne i at udveksle lister over tilbagekaldte certifikater, hvilket der er fastsat bestemmelser for i artikel 4, stk. 2, i forordning (EU) 2021/953.

(21) Når Kommissionen behandler personoplysninger i portalen for EU's digitale covidcertifikat, er den bundet af Kommissionens afgørelse (EU, Euratom) 2017/46 ([7]).

(22) I henhold til artikel 3, stk. 10, i forordning (EU) 2021/953 kan Kommissionen vedtage gennemførelsesretsakter, der fastlægger, at covid-19-certifikater udstedt af et tredjeland, med hvilket Unionen og medlemsstaterne har indgået en aftale om fri bevægelighed for personer, som giver de kontraherende parter mulighed for at begrænse en sådan fri bevægelighed af hensyn til folkesundheden på en ikkeforskelsbehandlende måde, og som ikke indeholder en mekanisme for indarbejdelse af EU-retsakter, svarer til dem, der er udstedt i overensstemmelse med denne forordning. På dette grundlag vedtog Kommissionen den 8. juli 2021 gennemførelsesafgørelse (EU) 2021/1126 ([8]) om ligestilling af covid-19-certifikater, der udstedes af Schweiz.

([5]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([7]) Kommissionen offentliggør yderligere oplysninger om sikkerhedsstandarder for alle Kommissionens informationssystemer på https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_da.

([8]) Kommissionens gennemførelsesafgørelse (EU) 2021/1126 af 8. juli 2021 om ligestilling af covid-19-certifikater, der udstedes af Schweiz, med certifikater, der udstedes i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/953 (EUT L 243 af 9.7.2021, s. 49).

(23) I henhold til artikel 8, stk. 2, i forordning (EU) 2021/953 kan Kommissionen vedtage gennemførelsesretsakter, der foreskriver, at covid-19-certifikater udstedt af et tredjeland i overensstemmelse med standarder og teknologiske systemer, der er interoperable med tillidsrammen for EU's digitale covidcertifikat, og som gør det muligt at kontrollere certifikatets ægthed, gyldighed og integritet, og som indeholder de data, der er anført i bilaget til forordningen, skal anses som at svare til EU's digitale covidcertifikater med henblik på at lette indehavernes udøvelse af deres ret til fri bevægelighed inden for Unionen. Som anført i betragtning 28 i forordning (EU) 2021/953 vedrører artikel 8, stk. 2, i nævnte forordning accept af certifikater udstedt af tredjelande til unionsborgere og deres familiemedlemmer. Kommissionen har allerede vedtaget flere sådanne gennemførelsesretsakter.

(24) For at undgå mangler i afsløringen af tilbagekaldte certifikater, der er omfattet af sådanne gennemførelsesretsakter, bør det også være muligt for tredjelande, hvis covid-19-certifikater anses for at være tilsvarende i henhold til artikel 3, stk. 10, og artikel 8, stk. 2, i forordning (EU) 2021/953, at indsende relevante lister over tilbagekaldte certifikater til portalen for EU's digitale covidcertifikat.

(25) Nogle tredjelandsstatsborgere, der er i besiddelse af et tilbagekaldt covid-19-certifikat udstedt af et tredjeland, hvis covid-19-certifikater er blevet anset for at være ækvivalente i henhold til forordning (EU) 2021/953, kan falde uden for anvendelsesområdet for enten nævnte forordning eller forordning (EU) 2021/954 på det tidspunkt, hvor en liste over tilbagekaldte certifikater, hvori deres certifikat optræder, genereres af det pågældende tredjeland. Om alle de tredjelandsstatsborgere, der er indehavere af tilbagekaldte certifikater, er omfattet af nogen af disse forordninger, kan imidlertid ikke vides på det tidspunkt, hvor et tredjeland genererer en liste over tilbagekaldte certifikater. Det er således ikke muligt at søge at udelukke personer, der ikke er omfattet af anvendelsesområdet for nogen af disse forordninger, på det tidspunkt, hvor disse landes lister over tilbagekaldte certifikater oprettes, og forsøg på at gøre dette vil medføre, at medlemsstaterne ikke vil være i stand til at opdage tilbagekaldte certifikater, som indehaves af tredjelandsstatsborgere, der rejser til Unionen for første gang. Selv de tilbagekaldte certifikater for disse tredjelandsstatsborgere vil dog blive kontrolleret af medlemsstaterne, når deres indehavere rejser til Unionen, og efterfølgende, når de rejser inden for Unionen. De tredjelande, hvis certifikater er blevet anset for at være tilsvarende i henhold til forordning (EU) 2021/953, er ikke involveret i forvaltningen af portalen og kan derfor ikke betragtes som fælles dataansvarlige.

(26) Derudover har EU's digitale covidcertifikatsystem vist sig at være det eneste covid-19-certifikatsystem, der fungerer i stor skala på internationalt plan. Som følge heraf har EU's digitale covidcertifikat fået stadig større global betydning og har bidraget til at håndtere pandemien på internationalt plan ved at fremme sikker international rejseaktivitet og den globale genopretning. I forbindelse med vedtagelsen af yderligere gennemførelsesretsakter i henhold til artikel 8, stk. 2, i forordning (EU) 2021/953 opstår der nye behov i forbindelse med udfyldelsen af EU's digitale covidcertifikat. I henhold til reglerne i gennemførelsesafgørelse (EU) 2021/1073 er efternavn et obligatorisk felt i certifikatets tekniske indhold. Det er nødvendigt at ændre dette krav for at fremme inklusion og interoperabilitet med andre systemer, da der i nogle tredjelande er personer uden efternavn. I tilfælde, hvor certifikatindehaverens navn ikke kan opdeles i to dele, bør navnet anføres i samme felt (efternavn eller fornavn) i EU's digitale covidcertifikat, som det ville være tilfældet med indehaverens rejse- eller identitetsdokument. Denne ændring vil også i højere grad bringe certifikaternes tekniske indhold i overensstemmelse med de gældende specifikationer for maskinlæsbare rejsedokumenter, som Organisationen for International Civil Luftfart har offentliggjort.

(27) Gennemførelsesafgørelse (EU) 2021/1073 bør derfor ændres.

(28) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav en udtalelse den 11. marts 2022.

(29) For at give medlemsstaterne og Kommissionen tilstrækkelig tid til at gennemføre de ændringer, der er nødvendige for at muliggøre udveksling af lister over tilbagekaldte certifikater via portalen for EU's digitale covidcertifikat, bør denne afgørelse begynde at finde anvendelse fire uger efter ikrafttrædelsen.

(30) De i denne afgørelse fastsatte foranstaltninger er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat i henhold til artikel 14 i forordning (EU) 2021/953 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

I gennemførelsesafgørelse (EU) 2021/1073 foretages følgende ændringer:

1) Som artikel 5a, 5b og 5c indsættes:

»*Artikel 5a*

Udveksling af lister over tilbagekaldte certifikater

1. Tillidsrammen for EU's digitale covidcertifikat skal muliggøre udveksling af lister over tilbagekaldte certifikater via den centrale portal for EU's digitale covidcertifikat (»portalen«) i overensstemmelse med de tekniske specifikationer i bilag I.

2. I tilfælde, hvor medlemsstaterne tilbagekalder EU's digitale covidcertifikater, kan de indsende lister over tilbagekaldte certifikater til portalen.

3. Hvis medlemsstaterne indsender lister over tilbagekaldte certifikater, fører udstedelsesmyndighederne en liste over tilbagekaldte certifikater.

4. Hvis personoplysninger udveksles via portalen, begrænses behandlingen til det, som er nødvendigt for at støtte udvekslingen af tilbagekaldelsesoplysninger. Sådanne personoplysninger må kun anvendes til at kontrollere tilbagekaldelsesstatus for EU's digitale covidcertifikater, der er udstedt inden for rammerne af forordning (EU) 2021/953.

5. De oplysninger, der indgives til portalen, skal omfatte følgende data i overensstemmelse med de tekniske specifikationer i bilag I:

a) de pseudonymiserede unikke certifikatidentifikatorer for tilbagekaldte certifikater

b) en udløbsdato for den indsendte liste over tilbagekaldte certifikater

6. Hvis en udstedelsesmyndighed tilbagekalder EU's digitale covidcertifikater, som den har udstedt i henhold til forordning (EU) 2021/953 eller forordning (EU) 2021/954, og har til hensigt at udveksle relevante oplysninger via portalen, skal den fremsende de oplysninger, der er omhandlet i stk. 5, i form af lister over tilbagekaldte certifikater til portalen i et sikkert format i overensstemmelse med de tekniske specifikationer i bilag I.

7. Udstedelsesmyndighederne skal så vidt muligt tilvejebringe en løsning med henblik på at underrette indehavere af tilbagekaldte certifikater om deres certifikaters tilbagekaldelsesstatus og årsagen til tilbagekaldelsen på tidspunktet for tilbagekaldelsen.

8. Portalen indsamler de modtagne lister over tilbagekaldte certifikater Den stiller værktøjer til rådighed med henblik på distribution af listerne til medlemsstaterne. Den sletter automatisk listerne i overensstemmelse med de udløbsdatoer, som den indberettende myndighed har angivet for hver indsendt liste.

9. De udpegede nationale myndigheder eller officielle organer i medlemsstaterne, der behandler personoplysninger i portalen, er fælles dataansvarlige for de behandlede oplysninger. De fælles dataansvarliges forskellige ansvarsområder er som angivet i bilag VI.

10. Kommissionen er databehandler for personoplysninger, der behandles i portalen. I sin egenskab af databehandler sikrer Kommissionen på vegne af medlemsstaterne sikkerheden i forbindelse med overførsel og lagring af personoplysninger i portalen og overholder databehandlerens forpligtelser som fastsat i bilag VII.

11. Kommissionen og fælles dataansvarlige afprøver, vurderer og evaluerer regelmæssigt effektiviteten af de tekniske og organisatoriske foranstaltninger, der skal garantere sikkerheden i forbindelse med behandling af personoplysninger i portalen.

Artikel 5b

Tredjelandes indsendelse af lister over tilbagekaldte certifikater

Tredjelande, der udsteder covid-19-certifikater, for hvilke Kommissionen har vedtaget en gennemførelsesretsakt i henhold til artikel 3, stk. 10, eller artikel 8, stk. 2, i forordning (EU) 2021/953, kan i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag I, indsende lister over tilbagekaldte covid-19-certifikater omfattet af en sådan gennemførelsesretsakt, som skal behandles af Kommissionen på vegne af de fælles dataansvarlige i portalen som beskrevet i artikel 5a.

Artikel 5c

Forvaltning af behandlingen af personoplysninger i den centrale portal for EU's digitale covidcertifikat

1. De fælles dataansvarliges beslutningsproces styres af en arbejdsgruppe, der nedsættes under det udvalg, der er omhandlet i artikel 14 i forordning (EU) 2021/953.

2. De udpegede nationale myndigheder eller officielle organer i medlemsstaterne, der er fælles dataansvarlige for de personoplysninger, der behandles i portalen, skal udpege repræsentanter til den nævnte arbejdsgruppe.«

2) Bilag I ændres som anført i bilag I til nærværende afgørelse

3) Bilag V ændres som anført i bilag II til nærværende afgørelse

4) Teksten i bilag III til nærværende afgørelse indsættes som bilag VI

5) Teksten i bilag IV til nærværende beslutning indsættes som bilag VII.

Artikel 2

Denne afgørelse træder i kraft på tredjedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den finder anvendelse fra fire uger efter fra sin ikrafttræden.

Udfærdiget i Bruxelles, den 21. marts 2022.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

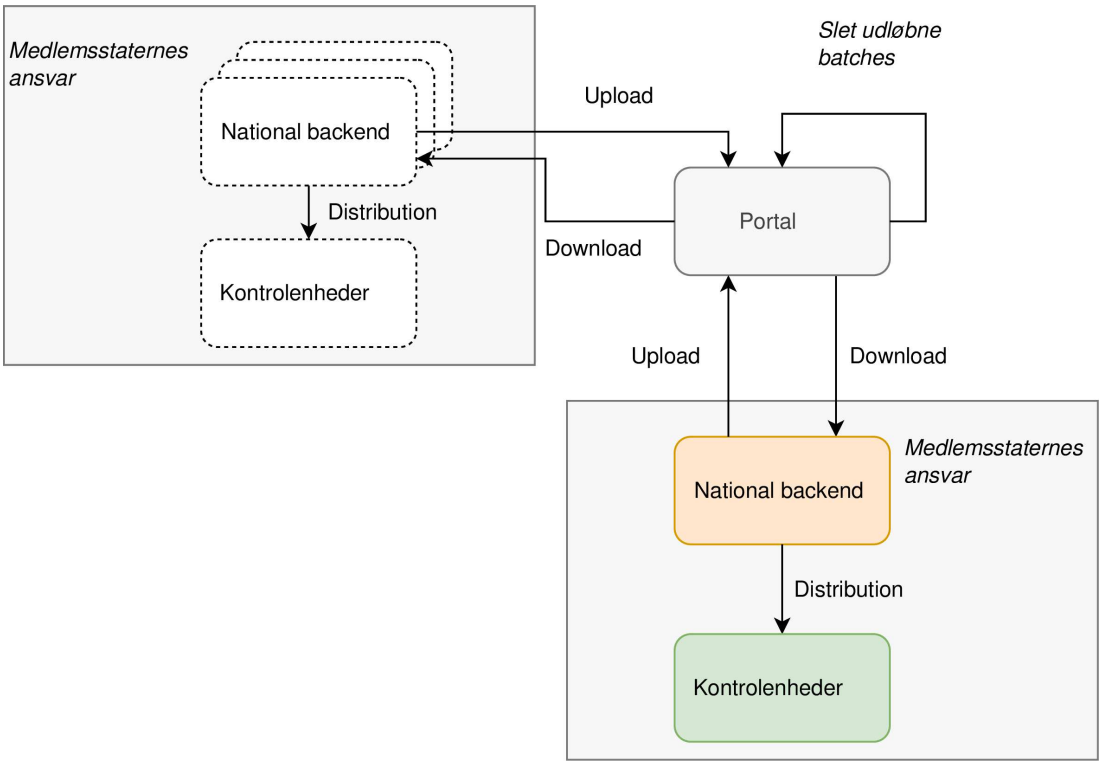
BILAG I

I bilag I til gennemførelsesafgørelse (EU) 2021/1073 indsættes følgende som afsnit 9:

»9. **TILBAGEKALDELSESLØSNING**

9.1. **Tilvejebringelse af lister over tilbagekaldte covidcertifikater**

Portalen tilvejebringer slutpunkter og funktionaliteter til at føre og forvalte lister over tilbagekaldte certifikater:



9.2. **Tillidsmodel**

Alle forbindelser etableres via standardtillidsmodellen for EU's digitale covidcertifikat (DCCG) ved hjælp af NB_{TLS}- og NB_{UP}-certifikater (se administration af certifikater). Alle oplysninger pakkes og uploades af CMS-meddelelser for at sikre integriteten.

9.3. **Batchudformning**

9.3.1. *Batch*

Hver liste over tilbagekaldte certifikater skal indeholde en eller flere indkodninger og være pakket i batches, som indeholder et sæt hashværdier og deres metadata. En batch er uforanderlig og definerer en udløbsdato, på hvilken batchen kan slettes. Udløbsdatoen for alle elementer i batchen skal være nøjagtigt den samme, hvilket betyder, at batchene skal grupperes efter udløbsdato og signeret DSC. Hver batch må maksimalt indeholde 1 000 indkodninger. Hvis en liste over tilbagekaldte certifikater indeholder mere end 1 000 indkodninger, skal der oprettes flere batches. En indkodning må kun optræde i ét batch. Batchen skal pakkes i en CMS-struktur og underskrives med det uploadende lands NB_{UP}-certifikat.

9.3.2. *Batchindeks*

Når der genereres en batch, tildeles den en unik identifikator af portalen og tilføjes automatisk til indekset. Batchindekset sorteres efter ændringsdato i stigende kronologisk rækkefølge.

9.3.3. *Portalens funktionsmåde*

Portalen behandler batches af tilbagekaldelser uden at foretage ændringer: Den kan hverken ajourføre, fjerne eller tilføje oplysninger til batchene. Batchene videresendes til samtlige autoriserede lande (se kapitel 9.6).

Portalen holder automatisk øje med batchenes udløbsdato og fjerner batches, der er udløbet. Når en batch slettes, sender portalen svaret »HTTP 410 Gone« for den slettede batchs URL. Batchen optræder derfor i batchindekset som »slettet«.

9.4. **Hashværdityper**

Listen over tilbagekaldte certifikater indeholder hashværdier, der kan repræsentere forskellige tilbagekaldelsestyper/-attributter. Disse typer eller attributter skal angives ved tilvejebringelsen af listerne over tilbagekaldte certifikater. De gængse typer er:

Type	Attribut	Hashberegning
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

Det er kun de første 128 bits af de hashværdier, der er kodet som Base64-strenge, som samles i batches og bruges til identifikation af de tilbagekaldte covidcertifikater ([1]).

9.4.1. *Hashværditype: SHA256(DCC Signature)*

I dette tilfælde beregnes hashværdien ud fra bytesene for signaturen COSE_SIGN1, som kommer fra CWT. For så vidt angår RSA-signaturer vil hele signaturen blive brugt som input. Formlen for certifikater, der er signeret med ECDSA, bruger værdien r som input:

SHA256(r)

[kræves for alle nye implementeringer]

9.4.2. *Hashværditype: SHA256(UCI)*

I dette tilfælde beregnes hashværdien ud fra UCI-strengen, der er kodet i UTF-8 og konverteret til en byte-array.

[forældet ([2]), men supporteres med henblik på bagudkompatibilitet]

9.4.3. *Hashværditype: SHA256(Issuing CountryCode+UCI)*

I dette tilfælde er landekoden indkodet som UTF-8-streng, der er sammenkædet med UCI'en kodet med en UTF-8-streng. Dette konverteres efterfølgende til en byte-array og bruges som input til hashfunktionen.

[forældet[2], men supporteres med henblik på bagudkompatibilitet]

9.5. **API-struktur**

9.5.1. *API til indkodning af tilbagekaldelser*

9.5.1.1. Formål

API'en leverer indkodninger i listen over tilbagekaldte certifikater i batches, inklusiv et batchindeks.

9.5.1.2. Slutpunkter

([1]) Se ligeledes 9.5.1.2 for de detaljerede API-beskrivelser.
([2]) Forældet betyder, at dette element ikke skal tages i betragtning i forbindelse med nye implementeringer, men at det skal supporteres for eksisterende implementeringer i en velafgrænset periode.

9.5.1.2.1. Slutpunkt for download af batchliste

Slutpunkterne har en enkel struktur og returnerer en liste over batches med en lille wrapper med metadata. Batchene sorteres efter *dato* i *stigende (kronologisk)* rækkefølge:

/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
        }, ..
        ]
}
```

Bemærkninger: Resultatet er som standard begrænset til 1 000. Hvis flaget »more« er sat til sandt, betyder det, at flere batches kan downloades. For at downloade yderligere elementer skal klienten sætte headeren If-Modified-Since til en dato, som ikke ligger før den sidst modtagne indkodning.

Svaret indeholder en JSON-array med følgende struktur:

Felt	Definition
more	Et boolesk flag, som angiver, at der findes flere batches.
batches	Array med eksisterende batches.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Landekode ISO 3166
date	ISO 8601 Dato UTC. Dato, hvor batchen blev tilføjet eller slettet.
deleted	boolean. Sandt hvis slettet. Når flaget sættes til »deleted«, kan indkodningen endeligt fjernes fra søgeresultaterne efter syv dage.

9.5.1.2.1.1. Svarkoder

Kode	Beskrivelse
200	Alt ok.
204	Intet indhold, hvis headeren »If-Modified-Since« ikke har noget match.

Anmodningsheader

Header	Obligatorisk	Beskrivelse
If-Modified-Since	Ja	Denne header indeholder den sidste downloadede dato, så kun de nyeste resultater vises. Ved første opkald bør headeren sættes til »2021-06-01T00:00:00Z«

9.5.1.2.2. Slutpunkt for download af batch

Batchen indeholder en liste over certifikatidentifikatorer:

/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 indeholder en CMS med en signatur, som skal svare til landets NB_{UP}-certifikat. Alle elementer i JSON-arrayen har følgende struktur:

Felt	Obligatorisk	Type	Definition
expires	Ja	String	Dato, hvor elementet kan fjernes. ISO8601 UTC-dato/-tid
country	Ja	String	Landekode ISO 3166
hashType	Ja	String	Hashtype brugt til indkodningerne (se Hashtyper)
entries	Ja	JSON Object Array	Se tabellen Indkodninger
kid	Ja	String	base64-kodet KID for den DSC, der er brugt til signatur af det digitale covidcertifikat. Hvis KID ikke er kendt, kan strengen `UNKNOWN_KID` (eksklusiv `) anvendes.

Bemærk:

— Batches skal grupperes efter udløbsdato og DSC. Alle elementer skal udløbe samtidigt og være signeret med den samme nøgle.

— Udløbsdatoen er angivet i UTC-dato/-tid, fordi EU-DCC er et globalt system, og der skal anvendes en entydig tidsangivelse.

— Udløbsdatoen for et permanent tilbagekaldt digitalt covidcertifikat sættes til udløbsdatoen for den tilsvarende DSC, der er brugt til at signere covidcertifikatet, eller til udløbstidspunktet for det tilbagekaldte digitale covidcertifikat (i så tilfælde skal den anvendte NumericDate-/Epoch-tidsangivelse behandles, som om det var UTC-tid).

— National backend (*NB*) skal fjerne elementer fra listen over tilbagekaldte certifikater, når **udløbsdatoen** nås.

— *NB* kan fjerne elementer fra deres lister over tilbagekaldte certifikater i tilfælde af, at den **KID**, der er brugt til signere det digitale covidcertifikat, tilbagekaldes.

9.5.1.2.2.1. Indkodninger

Felt	Obligatorisk	Type	Definition
hash	Ja	String	Første 128 bits af hashværdien SHA256 kodet som en Base64-streng

Bemærk: Indkodningsobjektet indeholder p.t. kun en hashværdi, men for at være kompatibel med fremtidige ændringer, er der valgt et objekt frem for en JSON-array.

9.5.1.2.2.2. Svarkoder

Kode	Beskrivelse
200	Alt ok.
410	Batch slettet. Batch kan slettes i den nationale backend.

9.5.1.2.2.3. Svarheader

Header	Beskrivelse
ETag	Batch ID.

9.5.1.2.3. Slutpunkt for upload af batch

Upload foretages med samme slutpunkt via verbet DELETE:

/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 signeres ved hjælp af NB_{UP}-certifikatet. Portalen verificerer, at signaturen er sat af NB_{UP}-certifikatet for det pågældende *land*. Hvis signaturen ikke består tjekket, kan uploadet ikke gennemføres.

BEMÆRK: Hver batch er uforanderlig og kan ikke ændres efter upload. Den kan dog godt slettes. ID'en for hver batch lagres, og upload af en ny batch med samme ID afvises.

9.5.1.2.4. Slutpunkt for sletning af batches

En batch kan slettes med samme slutpunkt via verbet DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

eller — af kompatibilitetsårsager — til følgende slutpunkt med verbet POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

9.6. **API-beskyttelse/databeskyttelsesforordningen**

I dette afsnit præciseres foranstaltninger, som skal sikre, at implementeringen overholder bestemmelserne i forordning (EU) 2021/953 for så vidt angår behandling af personoplysninger.

9.6.1. *Eksisterende autentificering*

Portalen anvender p.t. NB_{TLS}-certifikatet til at autentificere de lande, der opretter forbindelse til portalen. Denne autentificering kan bruges til at fastslå identiteten på det land, der er forbundet til portalen. Denne identitet kan efterfølgende bruges til adgangskontrol.

9.6.2. *Adgangskontrol*

For lovligt at kunne behandle personoplysninger skal portalen indføre en mekanisme til adgangskontrol.

Portalen benytter en adgangskontrolliste kombineret med et rollebaseret sikkerhedssystem. Systemet skal indeholde to tabeller: En tabel, som beskriver hvilke roller, der kan udføre hvilke operationer med hvilke ressourcer, og en anden tabel, som beskriver, hvilke roller er tildelt hvilke brugere.

For at gennemføre de i dette dokument fastsatte kontroller kræves der tre roller, som er:

RevocationListReader

RevocationUploader

RevocationDeleter

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationListReader; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationUploader; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

POST/revocation-list

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationDeleter; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Portalen skal tilvejebringe en pålidelig metode, hvorved administratorer kan forvalte de roller, der er knyttet til brugerne, på en sådan måde at det reducerer risikoen for menneskelige fejl og ikke udgør en byrde for de funktionelle administratorer.«

BILAG II

Afsnit 3 i bilag V til gennemførelsesafgørelse (EU) 2021/1073 affattes således:

»3. ***Fælles strukturer og generelle krav***

EU's digitale covidcertifikater udstedes ikke, hvis ikke alle datafelter grundet manglende oplysninger kan udfyldes korrekt i overensstemmelse med nærværende specifikation. **Dette påvirker ikke medlemsstaternes forpligtelse til at udstede digitale covidcertifikater.**

Oplysningerne i alle felter kan udfyldes ved anvendelse af det fulde sæt UNICODE 13.0-tegn kodet i UTF-8, medmindre der er specifikke begrænsninger af værdisættene eller et smallere sæt tegn.

Den fælles struktur skal være som følger:

»JSON«:{

»ver«:<oplysninger om version>,

»nam«:{

<oplysninger om navn>

},

»dob«:<fødselsdato>,

»v« eller »t« eller »r«: [

{<oplysninger om vaccinedosis, test eller restitution, én indkodning>}

]

}

Detaljerede oplysninger om individuelle grupper og felter følger i nedenstående afsnit.

Hvis reglerne foreskriver, at et felt skal springes over, betyder det, at indholdet skal være tomt, og at hverken feltets navn eller værdi må optræde i indholdet.

3.1. ***Version***

Oplysninger om version skal fremgå. Versioneringen følger Semantic Versioning (semver: https://semver.org). Den version, der bruges, skal det være en af de offentliggjorte versioner (nuværende eller tidligere offentliggjort version). Se afsnit JSON Schema location for yderligere oplysninger.

Felt-ID	Feltnavn	Instrukser
ver	Version af skema	Skal svare til identifikatoren for den version af skemaet, der anvendes til udarbejdelse af EU's digitale covidcertifikat. Eksempel: »ver«:»1.3.0«

3.2. ***Personens navn og fødselsdato***

Personens navn er personens fulde officielle navn, der svarer til det navn, der fremgår af rejsedokumenter. Strukturens identifikator er *nam*. Præcis 1 (ét) navn skal angives.

Felt-ID	Feltnavn	Instrukser
nam/fn	Efternavn(e)	Indehavers efternavn(e). Hvis indehaveren ikke har noget efternavn, men har et fornavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, indeholdende alle efternavne. I tilfælde af flere efternavne skal disse adskilles med mellemrum. Kombinerede navne, herunder med bindestreger eller lignende tegn, skal imidlertid ikke ændres.

		Eksempler: »fn«:»Musterfrau-Gößinger« »fn«:»Musterfrau-Gößinger Müller«
nam/fnt	Standardiseret/ standardiserede efternavn(e)	Indehaverens efternavn(e) translittereret efter samme regel som den, der er brugt til indehaverens maskinlæsbare rejsedokumenter (såsom de regler, der er fastsat i ICAO-dokument 9303, del 3). Hvis indehaveren ikke har noget efternavn, men har et fornavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, udelukkende indeholdende tegnene A-Z og <. Maksimal længde: 80 tegn (jf. ICAO-specifikation 9303). Eksempler: »fnt«:»MUSTERFRAU<GOESSINGER« »fnt«:»MUSTERFRAU<GOESSINGER<MUELLER«
nam/gn	Fornavn(e)	Fornavn(e) på indehaveren. Hvis indehaveren ikke har noget fornavn, men har et efternavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, indeholdende alle fornavne. I tilfælde af flere fornavne skal disse adskilles med mellemrum. Eksempel: »gn«:»Isolde Erika«
nam/gnt	Standardiseret/ standardiserede fornavn(e)	Indehaverens fornavn(e) translittereret efter samme regel som den, der er brugt til indehaverens maskinlæsbare rejsedokumenter (såsom de regler, der er fastsat i ICAO-dokument 9303, del 3). Hvis indehaveren ikke har noget fornavn, men har et efternavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, udelukkende indeholdende tegnene A-Z og <. Maksimal længde: 80 tegn. Eksempel: »gnt«:»ISOLDE<ERIKA«
dob	Fødselsdato	Fødselsdato på indehaveren af EU's digitale covidcertifikat. Fuldstændig eller delvis dato uden klokkeslæt, begrænset til intervallet fra 1900-01-01 til 2099-12-31. Præcis 1 (ét) ikketomt felt skal angives, hvis den fuldstændige eller delvise fødselsdato er kendt. Hvis fødselsdatoen ikke er kendt, heller ikke delvist, skal feltet udfyldes med en tom streng »«. Dette bør stemme overens med oplysningerne i rejsedokumenterne. Et af de følgende ISO 8601-formater skal anvendes, hvis fødselsdatoen er kendt. Andre muligheder understøttes ikke. ÅÅÅÅ-MM-DD ÅÅÅÅ-MM ÅÅÅÅ (Kontrolapplikationen kan vise manglende dele af fødselsdatoen ved at anvende XX-reglen ligesom i maskinlæsbare rejsedokumenter, f.eks. 1990-XX-XX.) Eksempler: »dob«:»1979-04-14« »dob«:»1901-08« »dob«:»1939« »dob«:»«

3.3. ***Grupper for oplysninger, der er specifikke for certifikattypen***

JSON-skemaet understøtter tre grupper af indkodninger, der omfatter oplysninger, som er specifikke for certifikattypen. Hvert digitalt covidcertifikat skal indeholde præcis 1 (én) gruppe. Tomme grupper er ikke tilladt.

Gruppeidentifikator	**Gruppens navn**	**Indkodninger**
v	Vaccinationsgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver 1 (én) vaccinedosis (én dosis).
t	Testgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver 1 (ét) et testresultat.
r	Restitutionsgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der beskriver 1 (én) oplysning om restitution.«

BILAG III

»BILAG VI

MEDLEMSSTATERNES ANSVAR SOM FÆLLES DATAANSVARLIGE FOR PORTALEN FOR EU'S DIGITALE COVIDCERTIFIKAT FOR SÅ VIDT ANGÅR UDVEKSLING AF LISTER OVER TILBAGEKALDTE CERTIFIKATER

AFSNIT 1

Underafsnit 1

Ansvarsfordeling

(1) De fælles dataansvarlige behandler personoplysninger via tillidsrammens portal i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag I.

(2) Medlemsstaternes udstedende myndigheder forbliver de eneste dataansvarlige for indsamling, anvendelse, offentliggørelse og enhver anden form for behandling af tilbagekaldelsesoplysninger uden for portalen, herunder for den procedure, der fører til tilbagekaldelse af et certifikat.

(3) Hver dataansvarlig er ansvarlig for at behandle personoplysninger i tillidsrammens portal i overensstemmelse med artikel 5, 24 og 26 i den generelle forordning om databeskyttelse.

(4) Hver dataansvarlig opretter et kontaktpunkt med en funktionel mailboks, som anvendes til kommunikation mellem selve de fælles dataansvarlige og mellem de fælles dataansvarlige og databehandleren.

(5) En midlertidig undergruppe oprettet i overensstemmelse med artikel 14 i forordning (EU) 2021/953 skal have til opgave at undersøge alle spørgsmål, der opstår i forbindelse med udveksling af listerne over tilbagekaldte certifikater, og det fælles dataansvar for dertil knyttet behandling af personoplysninger, og at lette koordinerede instrukser til Kommissionen som databehandler. De fælles dataansvarliges beslutningsproces styres af denne arbejdsgruppe og af den forretningsorden, som gruppen vedtager. Grundlæggende gælder det, at en fælles dataansvarligs manglende deltagelse i et møde i denne arbejdsgruppe, som er meddelt mindst syv (7) dage før den skriftlige mødeindkaldelse, er ensbetydende med stiltiende enighed med resultaterne af dette møde i arbejdsgruppen. Enhver af de fælles dataansvarlige kan indkalde til møde i arbejdsgruppen.

(6) Instrukser til databehandleren sendes af et af de fælles dataansvarliges kontaktpunkter efter aftale med de øvrige fælles dataansvarlige, jf. arbejdsgruppens beslutningsproces som beskrevet i ovenstående punkt 5. Den fælles dataansvarlige, som udsteder instrukser, skal fremlægge disse for databehandleren på skrift og informere alle andre fælles dataansvarlige herom. Hvis det pågældende spørgsmål er så tilstrækkeligt tidskritisk, at det ikke er muligt at holde et møde i den arbejdsgruppe, der er omhandlet i ovenstående punkt 5, kan der alligevel udstedes en instruks, som dog kan annulleres af arbejdsgruppen. Denne instruks bør gives skriftligt, og alle de andre fælles dataansvarlige bør i den forbindelse informeres herom.

(7) Den arbejdsgruppe, der er nedsat i overensstemmelse med punkt 5, udelukker ikke den enkelte fælles dataansvarliges individuelle kompetence til at informere sin kompetente tilsynsmyndighed i overensstemmelse med artikel 33 og 24 i den generelle forordning om databeskyttelse. En sådan meddelelse kræver ikke de øvrige fælles dataansvarliges samtykke.

(8) Kun personer med tilladelse fra de udpegede nationale myndigheder eller officielle organer må tilgå de personoplysninger, der udveksles i tillidsrammens portal.

(9) Hver udstedende myndighed fører en fortegnelse over behandlingsaktiviteter under dens ansvarsområde. Det fælles dataansvar kan angives i fortegnelsen.

Underafsnit 2

Ansvar og roller i forbindelse med behandling af anmodninger fra og information af registrerede

(1) Hver dataansvarlig skal i sin rolle som udstedende myndighed over for fysiske personer, hvis certifikat(er), den har tilbagekaldt, (»de registrerede«) fremlægge oplysninger om den pågældende tilbagekaldelse og om behandling af deres personoplysninger i portalen for EU's digitale covidcertifikat med henblik på at støtte udvekslingen af lister over tilbagekaldte certifikater, jf. artikel 14 i den generelle forordning om databeskyttelse, medmindre dette viser sig at være umuligt eller vil indebære en uforholdsmæssig stor indsats.

(2) Hver dataansvarlig fungerer som kontaktpunkt for fysiske personer, hvis certifikater, den har tilbagekaldt, og behandler anmodninger vedrørende udøvelsen af registreredes rettigheder i overensstemmelse med den generelle forordning om databeskyttelse. Hvis en fælles dataansvarlig modtager en anmodning fra en registreret vedrørende et certifikat, der er udstedt af en anden fælles dataansvarlig, informerer den den registrerede om den ansvarlige fælles dataansvarliges identitet og kontaktoplysninger. De fælles dataansvarlige bistår efter anmodning fra en fælles dataansvarlig hinanden med behandlingen af registreredes anmodninger, og de svarer hinanden hurtigst muligt og under alle omstændigheder senest 1 måned efter at have modtaget en anmodning om bistand. Hvis en anmodning vedrører data indsendt af et tredjeland, skal den dataansvarlige, som modtager anmodningen, behandle anmodningen og informere den registrerede om identitet og kontaktoplysninger på tredjelandets udstedende myndighed.

(3) Hver dataansvarlig stiller indholdet af dette bilag, herunder de ordninger, der er fastlagt i punkt 1 og 2, til rådighed for de registrerede.

AFSNIT 2

Håndtering af sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden

(1) De fælles dataansvarlige bistår hinanden med identifikation og håndtering af eventuelle sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden, i forbindelse med behandlingen i portalen for EU's digitale covidcertifikat.

(2) De fælles dataansvarlige underretter især hinanden om følgende:

a) enhver potentiel eller reel risiko i forhold til adgangen til, fortroligheden for og/eller integriteten af de personoplysninger, der er genstand for behandling i tillidsrammens portal

b) ethvert brud på persondatasikkerheden, de sandsynlige konsekvenser af bruddet på persondatabeskyttelsen og en vurdering af risikoen for fysiske personers rettigheder og frihedsrettigheder samt alle foranstaltninger, der træffes for at håndtere bruddet på persondatasikkerheden og begrænse risikoen for fysiske personers rettigheder og frihedsrettigheder

c) enhver overtrædelse af de tekniske og/eller organisatoriske sikkerhedsforanstaltninger for behandlingsaktiviteterne i tillidsrammens portal.

(3) De fælles dataansvarlige anmelder, i overensstemmelse med artikel 33 og 34 i den generelle forordning om databeskyttelse eller efter anmeldelse fra Kommissionen, ethvert brud på persondatasikkerheden i forbindelse med behandlingsaktiviteterne i tillidsrammens portal til Kommissionen, til de kompetente tilsynsmyndigheder og, for så vidt det er påkrævet, til de registrerede.

(4) Hver udstedende myndighed for systemet for tidlig varsling og reaktion gennemfører passende tekniske og organisatoriske foranstaltninger, der har til formål at:

a) garantere og sikre tilgængelighed, integritet og fortrolighed af de fælles behandlede personoplysninger

b) beskytte personoplysninger i dens besiddelse mod uautoriseret eller ulovlig behandling, tab, anvendelse, offentliggørelse eller erhvervelse af eller adgang dertil

c) sikre, at adgangen til personoplysninger ikke offentliggøres eller gives til andre end modtagerne eller behandlerne.

AFSNIT 3

Konsekvensanalyse vedrørende databeskyttelse

(1) Hvis en dataansvarlig, for at overholde sine forpligtelser i henhold til artikel 35 og 36 i forordning (EU) 2016/679, har brug for oplysninger fra en anden dataansvarlig, sender førstnævnte dataansvarlige en specifik anmodning til den fællespostkasse, der er omhandlet i afsnit 1, underafsnit 1, punkt 4. Sidstnævnte gør sit bedste for at tilvejebringe de pågældende oplysninger.«

BILAG IV

»BILAG VII

KOMMISSIONENS ANSVAR SOM FÆLLES DATABEHANDLER FOR PORTALEN FOR EU'S DIGITALE COVIDCERTIFIKAT FOR SÅ VIDT ANGÅR STØTTE AF UDVEKSLINGEN AF LISTER OVER TILBAGEKALDTE CERTIFIKATER

Kommissionen skal:

(1) på vegne af medlemsstaterne etablere og sikre en sikker og pålidelig kommunikationsinfrastruktur, som støtter udvekslingen af de lister over tilbagekaldte certifikater, der indsendes til portalen for EU's digitale covidcertifikat.

(2) For at opfylde sine forpligtelser som databehandler for tillidsrammens portal kan Kommissionen inddrage tredjeparter som underdatabehandlere; Kommissionen skal underrette de fælles dataansvarlige om påtænkte ændringer vedrørende tilføjelse eller udskiftning af andre underdatabehandlere, således at de dataansvarlige får mulighed for i fællesskab at gøre indsigelse mod de pågældende ændringer. Kommissionen sikrer, at der gælder samme databeskyttelsesforpligtelser for disse underdatabehandlere som fastsat i denne afgørelse

(3) behandle personoplysningerne udelukkende efter dokumenterede instrukser fra de dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret; i så fald underretter Kommissionen de fælles dataansvarlige om dette retlige krav, inden oplysningerne behandles, medmindre den pågældende ret forbyder en sådan underretning af hensyn til væsentlige samfundsinteresser.

Kommissionens behandling indebærer følgende:

a) at autentificere nationale backend-servere på grundlag af nationale backend-servercertifikater

b) at modtage de data omhandlet i afgørelsens artikel 5a, stk. 3, der uploades af de nationale backend-servere, ved at stille en applikationsprogrammeringsgrænseflade til rådighed, som gør det muligt for nationale backend-servere at uploade de relevante data

c) at lagre data i portalen for EU's digitale covidcertifikat

d) at stille dataene til rådighed, så de kan downloades af de nationale backend-servere

e) at slette data efter deres udløbsdato eller efter instruks fra den dataansvarlige, der har indsendt dem

f) at slette eventuelle resterende data, efter at tjenesterne er ophørt, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

(4) træffe alle avancerede organisatoriske, fysiske og logiske sikkerhedsforanstaltninger for at vedligeholde portalen for EU's digitale covidcertifikat. Kommissionen skal med henblik herpå:

a) udpege en enhed, der er ansvarlig for sikkerhedsstyring på niveauet for portalen for EU's digitale covidcertifikat, kommunikere enhedens kontaktoplysninger til de fælles dataansvarlige og sikre, at enheden kan reagere på sikkerhedstrusler

b) påtage sig ansvaret for sikkerheden ved portalen for EU's digitale covidcertifikat, herunder foretage regelmæssige test, evalueringer og vurderinger af sikkerhedsforanstaltningerne

c) sikre, at alle, der får adgang til portalen for EU's digitale covidcertifikat, er underlagt kontraktlig, professionel eller lovbestemt tavshedspligt

(5) træffe alle nødvendige sikkerhedsforanstaltninger til at undgå at kompromittere driften af de nationale backend-servere. Kommissionen skal til dette formål fastlægge specifikke procedurer i tilknytning til forbindelsen fra backend-serverne til portalen for EU's digitale covidcertifikat. Dette omfatter:

a) risikovurderingsprocedure — til identificering og vurdering af mulige trusler mod systemet

b) audit- og kontrolprocedure til:

i. kontrol af overensstemmelse mellem de gennemførte sikkerhedsforanstaltninger og sikkerhedspolitik i anvendelse

ii. regelmæssig kontrol af integriteten af systemfiler, sikkerhedsparametre og udstedte tilladelser

iii. overvågning med henblik på afsløring af brud på sikkerheden og indtrængen

iv. gennemførelse af ændringer for at begrænse eksisterende sikkerhedsproblemer

v. fastsættelse af betingelser, under hvilke der gives tilladelse, herunder på anmodning fra dataansvarlige, og bidrage til udførelsen af uafhængige audit, herunder inspektioner, og gennemgang af sikkerhedsforanstaltninger på vilkår, der er i overensstemmelse med protokol (nr. 7) til TEUF vedrørende Den Europæiske Unions privilegier og immuniteter

c) ændring af kontrolproceduren til dokumentation og måling af virkningen af en ændring, før den gennemføres, og underretning af de fælles dataansvarlige om ændringer, der kan påvirke kommunikationen med og/eller sikkerheden i deres infrastrukturer

d) fastlæggelse af en vedligeholdelses- og reparationsprocedure til præcisering af bestemmelser og betingelser, som skal overholdes ved vedligeholdelse og/eller reparation af udstyr

e) fastlæggelse af en procedure for sikkerhedsrelaterede hændelser til fastlæggelse af rapporterings- og eskaleringsordningen, omgående underretning af de berørte dataansvarlige, så de kan underrette de nationale datatilsynsmyndigheder om brud på persondatasikkerheden og fastlæggelse af en disciplinær proces til håndtering af brud på sikkerheden

(6) træffe avancerede fysiske og/eller logiske sikkerhedsforanstaltninger for de faciliteter, som opbevarer udstyret til portalen for EU's digitale covidcertifikat, og for kontrollen af adgangen til logiske data og sikkerhed. Kommissionen skal med henblik herpå:

a) håndhæve den fysiske sikkerhed for at oprette særlige sikkerhedsområder og muliggøre afsløring af brud

b) kontrollere adgang til faciliteterne og vedligeholde et besøgsregister med henblik på sporing

c) sikre, at eksterne personer med adgang til området ledsages af behørigt bemyndigede medarbejdere

d) sikre, at udstyr ikke kan tilføjes, erstattes eller fjernes uden forudgående godkendelse fra de udpegede ansvarlige organer

e) kontrollere adgang fra og til de nationale backend-servere til tillidsrammens portal

f) sikre, at alle, der har adgang til portalen for EU's digitale covidcertifikat, identificeres og autentificeres

g) gennemgå godkendelsesrettighederne i forbindelse med adgang til portalen for EU's digitale covidcertifikat, i tilfælde af at et brud på sikkerheden har betydning for denne infrastruktur

h) fastholde integriteten i de oplysninger, der overføres via portalen for EU's digitale covidcertifikat

i) gennemføre tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre uautoriseret adgang til personoplysninger

j) om nødvendigt gennemføre foranstaltninger for at blokere uautoriseret adgang til portalen for EU's digitale covidcertifikat fra de udstedende myndigheders domæne (dvs. blokere en lokation/IP-adresse)

(7) træffe foranstaltninger til beskyttelse af sit domæne, herunder fjerne forbindelser, hvis der er væsentlig afvigelse fra principper og koncepter for kvalitet og sikkerhed

(8) opstille en risikostyringsplan i forbindelse med sit ansvarsområde

(9) overvåge — i realtid — udførelsen af alle servicekomponenter af sine tjenester i tillidsrammens portal, udarbejde regelmæssige statistikker og føre registre

(10) yde støtte til alle tjenester i tillidsrammens portal på engelsk 24/7 via telefon, e-mail eller webportal og modtage opkald fra autoriserede personer: koordinatorer af portalen for EU's digitale covidcertifikat og deres respektive helpdeske, projektledere og udpegede personer fra Kommissionen.

(11) bistå de fælles dataansvarlige, i den udstrækning det er muligt og ved hjælp af passende tekniske og organisatoriske foranstaltninger, jf. artikel 12 i forordning (EU) 2018/1725, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III i den generelle forordning om databeskyttelse

(12) yde støtte til de fælles dataansvarlige ved at levere oplysninger vedrørende portalen for EU's digitale covidcertifikat for at gennemføre forpligtelserne i henhold til artikel 32, 33, 34, 35 og 36 i den generelle forordning om databeskyttelse

(13) sikre, at oplysninger, der behandles inden for portalen for EU's digitale covidcertifikat, er uforståelige for alle, der ikke har tilladelse til at tilgå faciliteten

(14) træffe alle relevante foranstaltninger for at forhindre, at operatører af den portalen for EU's digitale covidcertifikat har uautoriseret adgang til overførte oplysninger

(15) træffe foranstaltninger for at fremme interoperabiliteten og kommunikationen mellem de udpegede dataansvarlige for portalen for EU's digitale covidcertifikat

(16) føre en fortegnelse over de behandlingsaktiviteter, der foretages på vegne af de fælles dataansvarlige, i overensstemmelse med artikel 31, stk. 2, i forordning (EU) 2018/1725.«