# DECISÃO DE EXECUÇÃO (UE) 2022/483 DA COMISSÃO

## de 21 de março de 2022

## que altera a Decisão de Execução (UE) 2021/1073 que estabelece as especificações técnicas e regras para a execução do regime de confiança do Certificado Digital COVID da UE estabelecido pelo Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho

**(Texto relevante para efeitos do EEE)**

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho, de 14 de junho de 2021, relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE), a fim de facilitar a livre circulação durante a pandemia de COVID-19 ([1]), nomeadamente o artigo 9.º, n.º 1,

Considerando o seguinte:

(1) O Regulamento (UE) 2021/953 estabelece o Certificado Digital COVID da UE, que comprova que uma pessoa recebeu uma vacina contra a COVID-19, um resultado negativo no teste ou recuperou da infeção, para o efeito de facilitar o exercício do direito de livre circulação do titular do certificado durante a pandemia de COVID-19.

(2) O Regulamento (UE) 2021/954 do Parlamento Europeu e do Conselho ([2]) obriga os Estados-Membros a aplicar as regras estabelecidas no Regulamento (UE) 2021/953 aos nacionais de países terceiros não abrangidos pelo âmbito deste último regulamento, mas que permaneçam ou residam legalmente no seu território e tenham direito a viajar para outros Estados-Membros em conformidade com o direito da União.

(3) A Recomendação (UE) 2022/290 do Conselho, que altera a Recomendação (UE) 2020/912 relativa à restrição temporária das viagens não indispensáveis para a UE e ao eventual levantamento de tal restrição ([3]), prevê que os nacionais de países terceiros que pretendam efetuar viagens não indispensáveis de países terceiros para a UE devem estar na posse de um comprovativo válido de vacinação ou recuperação, como um Certificado Digital COVID da UE ou um certificado COVID-19 emitido por um país terceiro abrangido por um ato de execução adotado nos termos do artigo 8.º, n.º 2, do Regulamento (UE) 2021/953.

(4) Para que o Certificado Digital COVID da UE esteja operacional em toda a União, a Comissão adotou a Decisão de Execução (UE) 2021/1073 ([4]) que estabelece as especificações técnicas e regras para preencher, emitir e verificar com segurança os Certificados Digitais COVID da UE, assegurar a proteção dos dados pessoais, definir a estrutura comum do identificador único do certificado e emitir um código de barras válido, seguro e interoperável.

(5) O artigo 4.º do Regulamento (UE) 2021/953 incumbe a Comissão e os Estados-Membros de criar e manter um regime de confiança para o Certificado Digital COVID da UE. Este regime de confiança pode apoiar o intercâmbio bilateral de listas de revogação de certificados que contenham os identificadores únicos dos certificados revogados.

([1]) JO L 211 de 15.6.2021, p. 1.

([2]) Regulamento (UE) 2021/954 do Parlamento Europeu e do Conselho, de 14 de junho de 2021, relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE) no que respeita a nacionais de países terceiros que permaneçam ou residam no território dos Estados-Membros durante a pandemia de COVID-19 (JO L 211 de 15.6.2021, p. 24).

([3]) Recomendação (UE) 2022/290 do Conselho, de 22 de fevereiro de 2022, que altera a Recomendação (UE) 2020/912 relativa à restrição temporária das viagens não indispensáveis para a UE e ao eventual levantamento de tal restrição (JO L 43 de 24.2.2022, p. 79).

([4]) Decisão de Execução (UE) 2021/1073 da Comissão, de 28 de junho de 2021, que estabelece as especificações técnicas e regras para a execução do regime de confiança do Certificado Digital COVID da UE estabelecido pelo Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho (JO L 230 de 30.6.2021, p. 32).

(6) Em 1 de julho de 2021, entrou em funcionamento o portal do Certificado Digital COVID da UE (a seguir designado por «portal»), que é o elemento central do regime de confiança e permite a troca segura e fiável entre os Estados-Membros de chaves públicas utilizadas para verificar Certificados Digitais COVID da UE.

(7) O êxito da implantação em grande escala dos Certificados Digitais COVID da UE chamou a atenção dos autores de fraudes, que procuram encontrar formas de emitir certificados fraudulentos. Urge, por isso, revogar tais certificados fraudulentos. Além disso, os Estados-Membros podem revogar, a nível nacional, certos Certificados Digitais COVID da UE por razões médicas e de saúde pública; por exemplo, após constatação de que um lote de vacinas administradas era defeituoso.

(8) Embora o sistema do Certificado Digital COVID da UE permita revelar imediatamente certificados falsificados, não é possível detetar certificados autênticos emitidos ilegalmente, com base em documentação falsa ou acesso não autorizado, ou com intenção fraudulenta noutros Estados-Membros, a menos que as listas de certificados revogados geradas a nível nacional sejam trocadas entre os Estados-Membros. O mesmo se aplica aos certificados revogados por razões médicas e de saúde pública. A incapacidade das aplicações de verificação dos Estados-Membros para detetar certificados revogados por outros Estados-Membros constitui uma ameaça para a saúde pública e põe em causa a confiança dos cidadãos no sistema do Certificado Digital COVID da UE.

(9) Tal como referido no considerando 19 do Regulamento (UE) 2021/953, por razões médicas e de saúde pública e em caso de certificados emitidos ou obtidos de forma fraudulenta, os Estados-Membros deverão poder estabelecer e trocar com outros Estados-Membros, para efeitos do referido regulamento, listas de revogação de certificados em casos limitados, em especial no atinente a certificados que tenham sido emitidos erradamente, devido a fraude ou na sequência da suspensão de um lote de vacina contra a COVID-19 considerado defeituoso. Os Estados-Membros não poderão revogar certificados emitidos por outros Estados-Membros. As listas de revogação de certificados partilhadas não podem conter quaisquer dados pessoais, com exceção dos identificadores únicos dos certificados. Em especial, não podem incluir os motivos da revogação dos certificados.

(10) Além de informações gerais sobre a possibilidade de revogação de certificados e dos eventuais motivos para tal, a autoridade emitente competente deve informar de imediato os titulares de certificados revogados dessa revogação efetiva e dos motivos da mesma. No entanto, em alguns casos, e em especial no dos Certificados Digitais COVID da UE emitidos em papel, localizar o titular do certificado e informá-lo da revogação pode revelar-se impossível ou implicar um esforço desproporcionado. Os Estados-Membros não podem recolher dados pessoais, além dos necessários para o processo de emissão, com o único propósito de conseguirem informar os titulares de certificados caso estes sejam revogados.

(11) Assim, é necessário reforçar o regime de confiança do Certificado Digital COVID da UE, apoiando o intercâmbio bilateral de listas de revogação de certificados entre os Estados-Membros.

(12) A presente decisão não abrange a suspensão temporária de certificados para casos de utilização nacionais fora do âmbito do Regulamento Certificado Digital COVID da UE, por exemplo, em virtude de o titular de um certificado de vacinação testar positivo ao SARS-CoV-2. Não prejudica os procedimentos estabelecidos quanto à verificação das regras operacionais relativas à validade dos certificados.

(13) Embora haja diferentes arquiteturas viáveis, do ponto de vista técnico, para o intercâmbio de listas de revogação, o portal é a solução mais adequada, uma vez que limita as trocas de dados ao regime de confiança já estabelecido e minimiza simultaneamente o número de possíveis pontos de falha e de trocas entre Estados-Membros, em comparação com um sistema posto-a-posto alternativo.

(14) Assim, afigura-se oportuno reforçar o portal do Certificado Digital COVID da UE de maneira que facilite o intercâmbio seguro de Certificados Digitais COVID da UE revogados, para efeitos da verificação segura dos mesmos por via do portal. A este respeito, é necessário aplicar medidas de segurança adequadas para proteger os dados pessoais tratados no portal. Os Estados-Membros devem pseudonimizar os atributos dos certificados por intermédio de um valor de dispersão (*hash*) irreversível, a incluir nas listas de revogação de certificados, o que permitirá assegurar um elevado nível de proteção. Com efeito, deve considerar-se que os identificadores únicos são dados pseudonimizados para fins das operações de tratamento realizadas no âmbito do portal.

(15) Além disso, é necessário estabelecer disposições relativas ao papel dos Estados-Membros e da Comissão no respeitante ao intercâmbio de listas de revogação de certificados.

(16) O tratamento de dados pessoais dos titulares de certificados, efetuado sob a responsabilidade dos Estados-Membros ou de outras organizações públicas ou organismos oficiais dos Estados-Membros, deve cumprir o disposto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([5]). O tratamento de dados pessoais efetuado sob a responsabilidade da Comissão para efeitos de gestão e garantia da segurança do portal do Certificado Digital COVID da UE deve cumprir o disposto no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([6]).

(17) Os Estados-Membros, representados pelas autoridades nacionais ou organismos oficiais designados, determinam em conjunto a finalidade e os meios de tratamento de dados pessoais através do portal do Certificado Digital COVID da UE e constituem, por conseguinte, responsáveis conjuntos pelo tratamento. O artigo 26.º do Regulamento (UE) 2016/679 impõe uma obrigação aos responsáveis conjuntos por operações de tratamento de dados no sentido de que determinem, de modo transparente, as respetivas responsabilidades pelo cumprimento do regulamento. O referido artigo prevê igualmente a possibilidade de essas responsabilidades serem determinadas pela legislação da União ou do Estado-Membro à qual os responsáveis pelo tratamento estão sujeitos. O acordo a que se refere o artigo 26.º deve ser incluído como anexo III da presente decisão.

(18) O Regulamento (UE) 2021/953 atribui à Comissão a tarefa de prestar apoio aos referidos intercâmbios. A forma mais adequada de cumprir esse mandato consiste em coligir, em nome dos Estados-Membros, as listas de revogação de certificados enviadas. Por conseguinte, deve ser atribuído à Comissão um papel de subcontratante, para que apoie estes intercâmbios, facilitando a troca de listas por intermédio do portal do Certificado Digital COVID da UE em nome dos Estados-Membros.

(19) A Comissão, enquanto fornecedor de soluções técnicas e organizativas para o portal do Certificado Digital COVID da UE, trata os dados pessoais constantes das listas de revogação enviadas para o portal em nome dos Estados-Membros, que são responsáveis conjuntos pelo tratamento. Atua, portanto, como subcontratante destes. Nos termos do artigo 28.º do Regulamento (UE) 2016/679 e do artigo 29.º do Regulamento (UE) 2018/1725, o tratamento por um subcontratante é regulado por um contrato ou ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincula o subcontratante ao responsável pelo tratamento e especifica o tratamento. Assim, afigura-se necessário definir regras aplicáveis ao tratamento de dados por parte da Comissão enquanto subcontratante.

(20) Tal como referido no considerando 52 do Regulamento (UE) 2021/953, a tarefa de apoio atribuída à Comissão não implica a criação de uma base de dados central. Esta proibição visa evitar a criação de um repositório central de todos os Certificados Digitais COVID da UE emitidos e não impede os Estados-Membros de trocarem listas de revogação de certificados, algo que está expressamente previsto no artigo 4.º, n.º 2, do Regulamento (UE) 2021/953.

(21) Ao proceder ao tratamento de dados pessoais no âmbito do portal do Certificado Digital COVID da UE, a Comissão encontra-se vinculada pela Decisão (UE, Euratom) 2017/46 da Comissão ([7]).

(22) O artigo 3.º, n.º 10, do Regulamento (UE) 2021/953 habilita a Comissão a adotar um ato de execução que estabeleça que os certificados de COVID-19 emitidos por um país terceiro com o qual a União e os seus Estados-Membros tenham celebrado um acordo sobre a livre circulação de pessoas que permita às partes contratantes restringir essa livre circulação por motivos de saúde pública, de forma não discriminatória, e que não inclua um mecanismo de incorporação de atos jurídicos da União, sejam equivalentes aos certificados de COVID-19 emitidos nos termos do referido regulamento. Com base nessa disposição, a Comissão adotou, em 8 de julho de 2021, a Decisão de Execução (UE) 2021/1126 ([8]) que estabelece a equivalência dos certificados COVID-19 emitidos pela Suíça.

([5]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([6]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

([7]) A Comissão publica mais informações sobre as normas de segurança aplicáveis a todos os sistemas de informação da Comissão Europeia em https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

([8]) Decisão de Execução (UE) 2021/1126 da Comissão, de 8 de julho de 2021, que estabelece a equivalência dos certificados COVID-19 emitidos pela Suíça com os certificados emitidos em conformidade com o Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho (JO L 243 de 9.7.2021, p. 49).

(23) O artigo 8.º, n.º 2, do Regulamento (UE) 2021/953 habilita a Comissão a adotar um ato de execução que estabeleça que os certificados de COVID-19 emitidos por um país terceiro de acordo com normas e sistemas tecnológicos que sejam interoperáveis com o regime de confiança do Certificado Digital COVID da UE e que permitam verificar a autenticidade, a validade e a integridade dos certificados, e que contenham os dados indicados no anexo do referido regulamento, devem ser considerados equivalentes aos Certificados Digitais COVID da UE, para efeitos de facilitar o exercício do direito de livre circulação na União por parte dos titulares. Como referido no considerando 28 do Regulamento (UE) 2021/953, o artigo 8.º, n.º 2, desse regulamento diz respeito à aceitação de certificados emitidos por países terceiros a cidadãos da União e a membros das suas famílias. A Comissão já adotou vários atos de execução desse teor.

(24) A fim de evitar falhas na deteção de certificados revogados abrangidos por esses atos de execução, os países terceiros cujos certificados COVID-19 tenham sido considerados equivalentes ao abrigo do artigo 3.º, n.º 10, e do artigo 8.º, n.º 2, do Regulamento (UE) 2021/953 devem poder enviar, igualmente, listas de revogação de certificados pertinentes para o portal do Certificado Digital COVID da UE.

(25) Alguns nacionais de países terceiros, titulares de certificados COVID-19 revogados emitidos por um país terceiro cujos certificados COVID-19 tenham sido considerados equivalentes nos termos do Regulamento (UE) 2021/953, podem não estar abrangidos pelo âmbito desse regulamento ou do Regulamento (UE) 2021/954 no momento em que o país terceiro em causa gerar uma lista de revogação que inclua os seus certificados. No entanto, é impossível saber, no momento em que um país terceiro gera uma lista de revogação de certificados, se todos os nacionais de países terceiros titulares de certificados revogados estão abrangidos pelo âmbito de algum dos referidos regulamentos. Assim, não é viável excluir pessoas não abrangidas pelo âmbito de qualquer dos regulamentos no momento em que esses países geram listas de revogação de certificados, e os esforços nesse sentido fariam com que os Estados-Membros não conseguissem detetar certificados revogados detidos por nacionais de países terceiros que viajassem pela primeira vez para a União. Porém, os Estados-Membros continuariam a verificar igualmente os certificados revogados desses nacionais de países terceiros que viajassem para a União e, subsequentemente, no interior da União. Os países terceiros cujos certificados tenham sido considerados equivalentes nos termos do Regulamento (UE) 2021/953 não estão envolvidos na governação do portal, pelo que não são considerados responsáveis conjuntos pelo tratamento.

(26) Além disso, o sistema do Certificado Digital COVID da UE demonstrou ser o único sistema de certificados COVID-19 operacional em grande escala a nível internacional. Consequentemente, o Certificado Digital COVID da UE adquiriu uma importância crescente a nível mundial e contribuiu para combater a pandemia a nível internacional, facilitando as viagens internacionais seguras e a recuperação global. Durante o processo de adoção de novos atos de execução ao abrigo do artigo 8.º, n.º 2, do Regulamento (UE) 2021/953, emergiram outras questões relacionadas com o preenchimento do Certificado Digital COVID da UE. De acordo com as regras estabelecidas na Decisão de Execução (UE) 2021/1073, o apelido é um campo de preenchimento obrigatório no conteúdo técnico do certificado. É necessário alterar este requisito para promover a inclusão e a interoperabilidade com outros sistemas, uma vez que, em alguns países terceiros, há pessoas sem apelido. Se não for possível dividir o nome do titular do certificado em duas partes, aquele deve ser inserido no campo (apelido ou nome próprio) do Certificado Digital COVID da UE equivalente ao que seria preenchido no documento de viagem ou de identidade do titular. Esta alteração permitiria também alinhar melhor o conteúdo técnico dos certificados com as especificações da Organização da Aviação Civil Internacional atualmente em vigor relativas aos documentos de viagem de leitura ótica.

(27) A Decisão de Execução (UE) 2021/1073 deve, por conseguinte, ser alterada em conformidade.

(28) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 e emitiu parecer em 11 de março de 2022.

(29) Para que os Estados-Membros e a Comissão disponham de tempo suficiente para introduzirem as alterações necessárias para permitir o intercâmbio de listas de revogação de certificados por intermédio do portal do Certificado Digital COVID da UE, a presente decisão deve começar a ser aplicada quatro semanas após a sua entrada em vigor.

(30) As medidas estabelecidas na presente decisão estão em conformidade com o parecer do comité criado nos termos do artigo 14.º do Regulamento (UE) 2021/953,

ADOTOU A PRESENTE DECISÃO:

*Artigo 1.º*

A Decisão de Execução (UE) 2021/1073 é alterada do seguinte modo:

1) são inseridos os seguintes artigos 5.º-A, 5.º-B e 5.º-C:

«*Artigo 5.º-A*

**Intercâmbio de listas de revogação de certificados**

1. O regime de confiança do Certificado Digital COVID da UE permite o intercâmbio de listas de revogação de certificados por intermédio do portal central do Certificado Digital COVID da UE (a seguir designado por "portal"), em conformidade com as especificações técnicas constantes do anexo I.

2. Sempre que os Estados-Membros revoguem Certificados Digitais COVID da UE, podem enviar listas de revogação de certificados para o portal.

3. Se os Estados-Membros enviarem listas de revogação de certificados, as autoridades emitentes devem manter uma lista dos certificados revogados.

4. Sempre que sejam trocados dados pessoais por intermédio do portal, o tratamento dos mesmos limita-se à finalidade de apoiar o intercâmbio de informações sobre a revogação. Esses dados pessoais só podem ser utilizados para efeitos de verificação do estado de revogação de Certificados Digitais COVID da UE emitidos no âmbito do Regulamento (UE) 2021/953.

5. As informações enviadas para o portal devem incluir os seguintes dados, em conformidade com as especificações técnicas constantes do anexo I:

a) os identificadores únicos dos certificados revogados, pseudonimizados;

b) a data de expiração da lista de revogação de certificados enviada;

6. Se uma autoridade emitente revogar Certificados Digitais COVID da UE por si emitidos nos termos do Regulamento (UE) 2021/953 ou do Regulamento (UE) 2021/954 e pretender trocar informações pertinentes por intermédio do portal, deve transmitir as informações referidas no n.º 5 sob a forma de listas de revogação de certificados enviadas para o portal num formato seguro, em conformidade com as especificações técnicas constantes do anexo I.

7. As autoridades emitentes devem, na medida do possível, encontrar uma solução que permita informar os titulares de certificados revogados do estado de revogação desses certificados, bem como dos motivos da revogação no momento da mesma.

8. O portal colige as listas de revogação de certificados recebidas e fornece ferramentas para as distribuir aos Estados-Membros. As listas são apagadas automaticamente, em conformidade com as datas de expiração indicadas para cada lista enviada pelas autoridades pertinentes.

9. As autoridades nacionais ou os organismos oficiais designados pelos Estados-Membros que tratam dados pessoais no portal são responsáveis conjuntos pelo tratamento desses dados. As responsabilidades respetivas dos responsáveis conjuntos pelo tratamento são atribuídas em conformidade com o anexo VI.

10. A Comissão é o subcontratante de dados pessoais tratados no portal. Na sua qualidade de subcontratante em nome dos Estados-Membros, a Comissão assegura a segurança da transmissão e do alojamento de dados pessoais no portal e cumpre as obrigações do subcontratante estabelecidas no anexo VII.

11. A Comissão e os responsáveis conjuntos pelo tratamento testam, analisam e avaliam periodicamente a eficácia das medidas técnicas e organizativas adotadas para garantir a segurança do tratamento de dados pessoais no portal.

*Artigo 5.º-B*

**Envio de listas de revogação de certificados por países terceiros**

Os países terceiros que emitam certificados COVID-19 relativamente aos quais a Comissão tenha adotado um ato de execução ao abrigo do artigo 3.º, n.º 10, ou do artigo 8.º, n.º 2, do Regulamento (UE) 2021/953 podem enviar listas de certificados COVID-19 revogados abrangidos por esse ato de execução, as quais a Comissão tratará em nome dos responsáveis conjuntos pelo tratamento no portal referido no artigo 5.º-A, em conformidade com as especificações técnicas estabelecidas no anexo I.

*Artigo 5.º-C*

**Governação do tratamento de dados pessoais no portal central do Certificado Digital COVID da UE**

1. O processo de tomada de decisões dos responsáveis conjuntos pelo tratamento é conduzido por um grupo de trabalho criado no âmbito do comité referido no artigo 14.º do Regulamento (UE) 2021/953.

2. As autoridades nacionais ou os organismos oficiais designados pelos Estados-Membros que tratam dados pessoais no portal na qualidade de responsáveis conjuntos pelo tratamento devem designar representantes para esse grupo.»;

2) o anexo I é alterado em conformidade com o anexo I da presente decisão;

3) o anexo V é alterado em conformidade com o anexo II da presente decisão;

4) o texto constante do anexo III da presente decisão é aditado como anexo VI;

5) o texto constante do anexo IV da presente decisão é aditado como anexo VII.

*Artigo 2.º*

A presente decisão entra em vigor no terceiro dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

A presente decisão é aplicável a partir de quatro semanas após a sua entrada em vigor.

Feito em Bruxelas, em 21 de março de 2022.

*Pela Comissão*
*A Presidente*
Ursula VON DER LEYEN

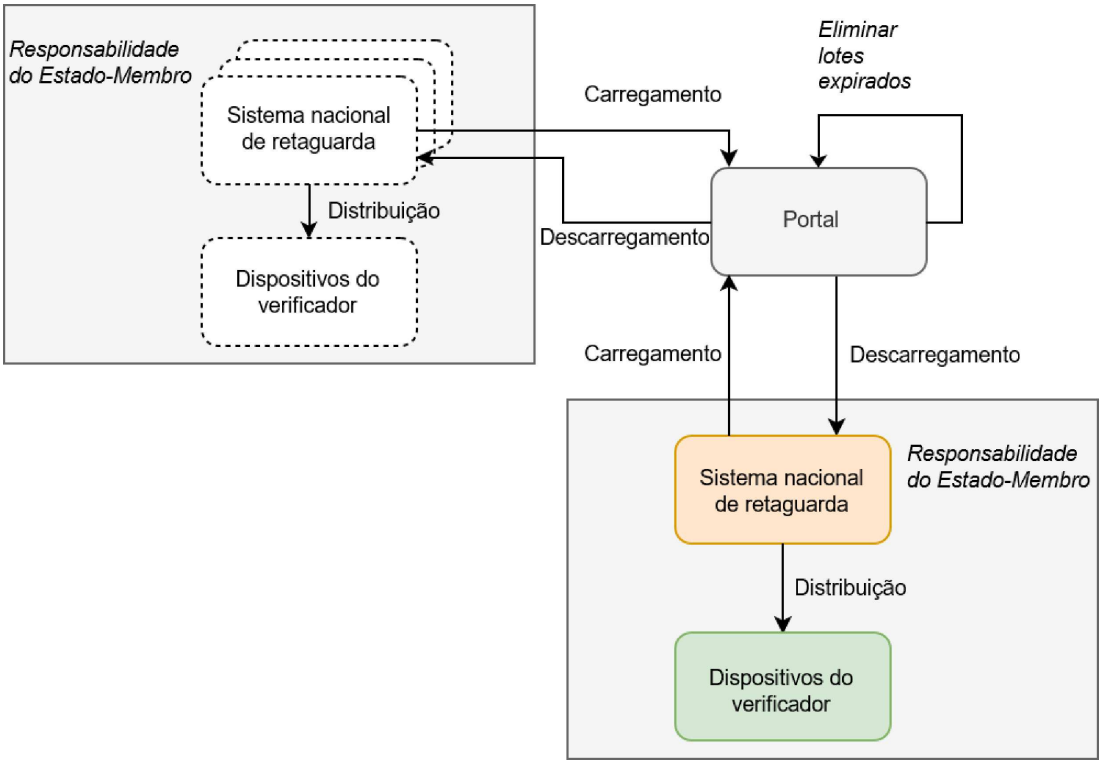
*ANEXO I*

Ao anexo I da Decisão de Execução (UE) 2021/1073 é aditado o seguinte ponto 9:

«9. **SOLUÇÃO DE REVOGAÇÃO**

9.1. **Envio de listas de revogação de Certificados Digitais COVID (*DRL — DCC Revocation List*)**

O portal fornece a funcionalidade e os pontos finais necessários para manter e gerir as listas de revogação:




9.2. **Modelo de confiança**

Todas as ligações são estabelecidas conforme o modelo de confiança normalizado do DCCG por intermédio dos certificados $NB_{TLS}$ e $NB_{UP}$ (ver disposições relativas à governação dos certificados). As informações são reunidas em pacotes e carregadas por via de mensagens CMS, de maneira que garanta a sua integridade.

9.3. **Criação de lotes**

9.3.1. *Lote*

Cada lista de revogação inclui uma ou várias entradas, que são agregadas em lotes (*batches*) que contêm um conjunto de valores de dispersão (*hashes*) e respetivos metadados. Um lote é imutável e define uma data de expiração que indica quando pode ser eliminado. A data de expiração tem de ser exatamente a mesma para todos os itens de um lote, pelo que os lotes têm de ser agregados por data de expiração e por assinatura dos DSC. Cada lote pode conter, no máximo, 1 000 entradas. Se uma lista de revogação incluir mais de 1 000 entradas, têm de ser criados vários lotes. Uma entrada individual pode ser incluída, no máximo, num lote. Cada lote é criado com uma estrutura CMS (sistema de gestão de conteúdo) e assinado pelo certificado $NB_{up}$ do país responsável pelo seu carregamento.

9.3.2. *Índice de lotes (batch index)*

Quando um lote é criado, o portal atribui-lhe um ID (identificador) único e adiciona-o automaticamente ao índice. O índice de lotes é disposto segundo a ordem cronológica ascendente das datas de modificação.

9.3.3. *Comportamento do portal*

O portal trata os lotes de revogação sem introduzir quaisquer alterações nos mesmos: não pode atualizar, suprimir ou acrescentar informações. Os lotes são enviados a todos os países autorizados (ver ponto 9.6).

O portal observa ativamente as datas de expiração dos lotes e remove os lotes expirados. Após a eliminação de um lote, o portal devolve uma resposta "HTTP 410 Gone" para o URL do lote eliminado. Assim, o lote é marcado no índice de lotes como "eliminado".

9.4. **Tipos de valores de dispersão**

A lista de revogação contém valores de dispersão que podem representar diferentes tipos/atributos de revogação. Estes tipos ou atributos são indicados aquando do envio das listas de revogação. Os tipos atualmente utilizados são os seguintes:

| Tipo | Atributo | Cálculo do valor de dispersão |
|---|---|---|
| SIGNATURE | DCC Signature | SHA256 de DCC Signature |
| UCI | UCI (Unique Certificate Identifier) | SHA256 de UCI |
| COUNTRYCODEUCI | Issuing Country Code + UCI | SHA256 de Issuing CountryCode + UCI |

**Apenas os primeiros 128 bits dos valores de dispersão codificados como cadeias (*strings*) de base64 são incluídos nos lotes e utilizados para identificar o DCC revogado** ([1]).

9.4.1. *Tipo de valor de dispersão: SHA256(DCC Signature)*

Neste caso, o valor de dispersão é calculado com base nos bytes da assinatura COSE_SIGN1 do CWT. As assinaturas RSA são integralmente utilizadas como entrada. A fórmula aplicável aos certificados assinados com EC-DSA utiliza o valor r como entrada:

SHA256(r)

[obrigatório para as novas implementações]

9.4.2. *Tipo de valor de dispersão: SHA256(UCI)*

Neste caso, o valor de dispersão é calculado com base na cadeia do UCI codificada em UTF-8 e convertida numa matriz de bytes (*byte array*).

[obsoleto ([2]), mas suportado para garantir compatibilidade com versões anteriores]

9.4.3. *Tipo de valor de dispersão: SHA256(Issuing CountryCode+UCI)*

Neste caso, o CountryCode (código de país) codificado como cadeia de UTF-8 é concatenado com o UCI codificado como cadeia de UTF-8. O resultado é convertido numa matriz de bytes e utilizado como entrada para a função de dispersão.

[obsoleto[2], mas suportado para garantir compatibilidade com versões anteriores]

9.5. **Estrutura da API**

9.5.1. *API para envio de entradas de revogação*

9.5.1.1. Finalidade

A API apresenta as entradas da lista de revogação em lotes, incluindo um índice de lotes.

9.5.1.2. Pontos finais

([1]) Para descrições pormenorizadas da API, consultar igualmente o ponto 9.5.1.2.

([2]) A indicação "obsoleto" significa que esta funcionalidade não deve ser considerada para novas implementações, mas deve ser suportada para implementações existentes durante um período bem definido.

9.5.1.2.1. Ponto final de descarregamento da lista de lotes

Os pontos finais seguem uma conceção simples, devolvendo uma lista de lotes com uma função de encapsulamento (*wrapper*) reduzida, que fornece metadados. Os lotes são dispostos segundo a ordem (*cronológica*) *ascendente* das *datas*:

/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
        }, ..
        ]
}
```

**Nota**: o resultado é limitado, por definição, a 1 000 entradas. Se a variável (*flag*) "more" devolver o valor "true" (verdadeiro), essa resposta indica que há mais lotes disponíveis para descarregamento. Para descarregar mais itens, o cliente tem de selecionar, no cabeçalho If-Modified-Since, uma data não anterior à da última entrada recebida.

A resposta contém uma matriz JSON com a seguinte estrutura:

| Campo | Definição |
|---|---|
| more | Variável booliana que indica se existem mais lotes. |
| batches | Matriz com os lotes existentes. |
| batchId | https://en.wikipedia.org/wiki/Universally_unique_identifier |
| country | Código ISO 3166 do país. |
| date | Data UTC (tempo universal coordenado) no formato ISO 8601. Data em que o lote foi adicionado ou eliminado. |
| deleted | *Boolean* [variável booliana]. "True" (verdadeiro) se o lote tiver sido eliminado. A entrada pode ser removida definitivamente dos resultados da consulta passados sete dias de esta variável assumir o valor de verdadeiro. |

9.5.1.2.1.1. Códigos de resposta

| Código | Descrição |
|---|---|
| 200 | Conteúdo apresentado normalmente. |
| 204 | Nenhum conteúdo apresentado, caso não haja correspondências com o conteúdo do cabeçalho "If-Modified-Since". |

*Cabeçalho do pedido*

| Cabeçalho | Obrigatório | Descrição |
|---|---|---|
| If-Modified-Since | Sim | Este cabeçalho contém a última data descarregada, para que sejam apresentados apenas resultados mais recentes. Numa primeira chamada à API, o cabeçalho deve estar definido do seguinte modo: "2021-06-01T00:00:00Z". |

9.5.1.2.2. Ponto final de descarregamento de lotes

Os lotes contêm uma lista de identificadores de certificados:

/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'

}, ..]

}

A resposta contém um CMS que inclui uma assinatura, a qual tem de corresponder ao certificado $NB_{UP}$ do país. Todos os itens da matriz JSON contêm a seguinte estrutura:

| Campo | Obrigatório | Tipo | Definição |
|---|---|---|---|
| expires | Sim | String | Data em que o item pode ser removido. Data/hora UTC no formato ISO 8601. |
| country | Sim | String | Código ISO 3166 do país. |
| hashType | Sim | String | Tipo do valor de dispersão das entradas apresentadas (ver Tipos de valores de dispersão) |
| entries | Sim | JSON Object Array | Ver quadro Entradas |
| kid | Sim | String | KID (identificador da chave) codificado em base64 do DSC utilizado para assinar o DCC. Se o KID for desconhecido, pode utilizar-se a cadeia "UNKNOWN_KID" (excluindo as aspas). |

*Notas*:

— Os lotes são agregados por data de expiração e por DSC, ou seja, todos os itens expiram em simultâneo e foram assinados usando a mesma chave;

— O prazo de expiração é uma data/hora no UTC, uma vez que o EU-DCC é um sistema global e é necessário utilizar uma hora inequívoca;

— A data de expiração de um DCC definitivamente revogado é fixada como a data de expiração do DSC correspondente utilizado para assinar o DCC ou como o prazo de expiração do DCC revogado (sendo que, neste caso, os prazos no formato NumericDate/epoch utilizados são tratados como estando no fuso horário UTC);

— Cabe aos sistemas nacionais de retaguarda (NB) remover itens das respetivas listas de revogação, uma vez atingida a data de **expiração**;

— Os N.B. podem remover itens das listas de revogação caso o **KID** utilizado para assinar o DCC seja revogado.

9.5.1.2.2.1. Entradas

| Campo | Obrigatório | Tipo | Definição |
|---|---|---|---|
| hash | Sim | String | Primeiros 128 bits do valor de dispersão SHA256 codificado como cadeia de base64 |

*Nota:* atualmente, o objeto das entradas contém apenas um valor de dispersão, mas, para garantir a compatibilidade com futuras alterações, optou-se por um objeto, em vez de uma matriz JSON.

9.5.1.2.2.2. Códigos de resposta

| Código | Descrição |
|---|---|
| 200 | Conteúdo apresentado normalmente. |
| 410 | O lote foi removido. O sistema nacional de retaguarda pode eliminar o lote. |

9.5.1.2.2.3. Cabeçalhos de resposta

| Cabeçalho | Descrição |
|---|---|
| ETag | ID do lote. |

9.5.1.2.3. Ponto final de carregamento de lotes

O carregamento é efetuado no mesmo ponto final, por via do método (ou verbo) de requisição 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'

}, ..]

}

O lote é assinado utilizando o certificado $NB_{UP}$. O portal verifica se o $NB_{UP}$ utilizado na assinatura corresponde ao *país* em causa. Se a verificação da assinatura falhar, o carregamento falhará igualmente.

*Nota*: todos os lotes são imutáveis e não podem ser alterados após o carregamento. No entanto, podem ser eliminados. O ID de cada lote eliminado é armazenado, sendo rejeitado o carregamento de um novo lote com o mesmo ID.

9.5.1.2.4. Ponto final de eliminação de lotes

Um lote pode ser eliminado no mesmo ponto final, por via do método (ou verbo) de requisição DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

ou, por questões de compatibilidade, no seguinte ponto final, por via do método (ou verbo) de requisição POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Proteção da API/RGPD**

A presente secção especifica medidas a aplicar para que a implementação cumpra as disposições do Regulamento (UE) 2021/953 no respeitante ao tratamento de dados pessoais.

9.6.1. *Autenticação existente*

Atualmente, o portal utiliza o certificado $NB_{TLS}$ para autenticar os países que se ligam ao portal. Esta autenticação pode ser utilizada para determinar a identidade do país ligado ao portal. Essa identidade pode ser subsequentemente utilizada para efeitos de controlo de acesso.

9.6.2. *Controlo de acesso*

Para poder tratar legalmente dados pessoais, o portal é obrigado a implantar um mecanismo de controlo de acesso.

O portal recorre a uma lista de controlo de acesso, combinada com uma política de segurança baseada em funções. Neste esquema, são mantidos dois quadros: um descreve as operações autorizadas a cada função e os recursos aos quais aquelas podem ser aplicadas; o outro descreve as funções atribuídas aos diferentes utilizadores.

Para executar os controlos exigidos pelo presente documento, são necessárias três funções, a saber:

RevocationListReader

RevocationUploader

RevocationDeleter

Os pontos finais a seguir indicados verificam se o utilizador tem a função de RevocationListReader; em caso afirmativo, o acesso é concedido; caso contrário, é devolvida uma mensagem HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Os pontos finais a seguir indicados verificam se o utilizador tem a função de RevocationUploader; em caso afirmativo, o acesso é concedido; caso contrário, é devolvida uma mensagem HTTP 403 Forbidden:

POST/revocation-list

Os pontos finais a seguir indicados verificam se o utilizador tem a função de RevocationDeleter; em caso afirmativo, o acesso é concedido; caso contrário, é devolvida uma mensagem HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

O portal proporciona igualmente um método fiável pelo qual os administradores podem gerir as funções atribuídas aos utilizadores, de modo que reduza a probabilidade de ocorrência de erros humanos, sem com isso sobrecarregar os administradores funcionais.»

*ANEXO II*

No anexo V da Decisão de Execução (UE) 2021/1073, o ponto 3 passa a ter a seguinte redação:

«3. ***Estruturas comuns e requisitos gerais***

Não é emitido um Certificado Digital COVID da UE se, devido à falta de informações, não for possível preencher corretamente todos os campos de dados em conformidade com a presente especificação. **Tal não deve ser entendido como afetando a obrigação de os Estados-Membros emitirem Certificados Digitais COVID da UE.**

As informações de todos os campos podem ser fornecidas utilizando o conjunto completo de carateres UNICODE 13.0 codificados em UTF-8, salvo se especificamente restringidos a conjuntos de valores ou a conjuntos de carateres mais reduzidos.

A estrutura comum é a seguinte:

*"JSON":{*

*"ver":<informação sobre a versão>,*

*"nam":{*

*<informação sobre o nome da pessoa>*

*},*

*"dob":<data de nascimento>,*

*"v" ou "t" ou "r":[*

*{<informação sobre a dose de vacinação ou o teste ou a recuperação, uma entrada>}*

]

*}*

Nas secções seguintes são fornecidas informações pormenorizadas sobre os diferentes grupos e campos.

Sempre que as regras indicarem que um campo deve ser ignorado, tal significa que o conteúdo deste deve permanecer vazio e que não é permitido inserir o nome ou o valor do campo.

3.1. ***Versão***

Devem ser fornecidas informações sobre a versão. A gestão das versões é efetuada segundo o Semantic Versioning (semver: https://semver.org). Em produção, deve ser uma das versões oficialmente publicadas (atuais ou oficialmente publicadas anteriormente). Para mais informações, ver o ponto relativo à localização do esquema (*Schema*) JSON.

| ID do campo | Nome do campo | Instruções |
|---|---|---|
| **ver** | Versão do esquema | Deve corresponder ao identificador da versão do esquema utilizada para produzir o EUDCC.<br>Exemplo:<br>"ver": "1.3.0" |

3.2. ***Nome e data de nascimento da pessoa***

O nome da pessoa é o nome oficial completo da pessoa, correspondente ao nome indicado nos documentos de viagem. O identificador da estrutura é *nam*. Deve ser fornecido exatamente 1 (um) nome de pessoa.

| ID do campo | Nome do campo | Instruções |
|---|---|---|
| **nam/fn** | Apelido(s) | Apelido(s) do titular<br>Se o titular não tiver apelidos e tiver um nome próprio, o campo deve ser ignorado.<br>Nos restantes casos, deve ser fornecido exatamente 1 (um) campo não vazio, com todos os apelidos nele incluídos. Em caso de apelidos múltiplos, estes devem ser separados por um espaço. Os nomes combinados que incluam hífenes ou carateres semelhantes devem, no entanto, permanecer iguais. |

| | | |
|---|---|---|
| | | Exemplos:<br>“fn”:“Musterfrau-Gößinger”<br>“fn”:“Musterfrau-Gößinger Müller” |
| **nam/fnt** | Apelido(s) normalizado(s) | Apelido(s) do titular transliterado(s) segundo a mesma convenção utilizada nos documentos de viagem de leitura automática do titular (por exemplo, as regras definidas na parte 3 do documento ICAO Doc 9303).<br>Se o titular não tiver apelidos e tiver um nome próprio, o campo deve ser ignorado.<br>Nos restantes casos, deve ser fornecido exatamente 1 (um) campo não vazio, incluindo apenas os carateres A-Z e <. Comprimento máximo: 80 carateres (de acordo com as especificações ICAO 9303).<br>Exemplos:<br>“fnt”:“MUSTERFRAU<GOESSINGER”<br>“fnt”:“MUSTERFRAU<GOESSINGER<MUELLER” |
| **nam/gn** | Nome(s) próprio(s) | Nome(s) próprio(s) do titular.<br>Se o titular não tiver nomes próprios e tiver um apelido, o campo deve ser ignorado.<br>Nos restantes casos, deve ser fornecido exatamente 1 (um) campo não vazio, com todos os nomes próprios nele incluídos. Em caso de nomes próprios múltiplos, estes devem ser separados por um espaço.<br>Exemplo:<br>“gn”:“Isolde Erika” |
| **nam/gnt** | Nome(s) próprio(s) normalizado(s) | Nome(s) próprio(s) do titular transliterado(s) segundo a mesma convenção utilizada nos documentos de viagem de leitura automática do titular (por exemplo, as regras definidas na parte 3 do documento ICAO Doc 9303).<br>Se o titular não tiver nomes próprios e tiver um apelido, o campo deve ser ignorado.<br>Nos restantes casos, deve ser fornecido exatamente 1 (um) campo não vazio, incluindo apenas os carateres A-Z e <. Comprimento máximo: 80 carateres.<br>Exemplo:<br>“gnt”:“ISOLDE<ERIKA” |
| **dob** | Data de nascimento | Data de nascimento do titular do DCC.<br>Data completa ou parcial sem hora, limitada ao intervalo compreendido entre 1900-01-01 e 2099-12-31.<br>Deve ser fornecido exatamente 1 (um) campo não vazio se a data de nascimento completa ou parcial for conhecida. Se a data de nascimento não for conhecida, mesmo parcialmente, o campo deve ser uma cadeia vazia: «». Estas informações devem corresponder às que constam dos documentos de viagem.<br>Se estiverem disponíveis informações sobre a data de nascimento, deve ser utilizado um dos seguintes formatos ISO 8601. Não são aceites outras opções.<br>YYYY-MM-DD<br>YYYY-MM<br>YYYY<br>(A aplicação de verificação pode mostrar as partes em faltam da data de nascimento utilizando a convenção XX como a utilizada nos documentos de viagem de leitura automática, por exemplo, 1990-XX-XX.)<br>Exemplos:<br>“dob”:“1979-04-14”<br>“dob”:“1901-08”<br>“dob”:“1939”<br>“dob”:”” |

3.3. ***Grupos para as informações específicas do tipo de certificado***

O esquema (*Schema*) JSON apoia três grupos de entradas que abrangem informações específicas do tipo de certificado. Cada EUDCC deve conter exatamente 1 (um) grupo. Não são permitidos grupos vazios.

| **Identificador do grupo** | **Nome do grupo** | **Entradas** |
|---|---|---|
| v | Grupo de vacinação | Se presente, deve conter exatamente 1 (uma) entrada que descreva exatamente 1 (uma) dose de vacinação (uma dose). |
| **t** | Grupo de teste | Se presente, deve conter exatamente 1 (uma) entrada que descreva exatamente 1 (um) resultado de teste. |
| **r** | Grupo de recuperação | Se presente, deve conter exatamente 1 (uma) entrada que descreva 1 (uma) declaração de recuperação.» |

*ANEXO III*

«*ANEXO VI*

**RESPONSABILIDADES DOS ESTADOS-MEMBROS ENQUANTO RESPONSÁVEIS CONJUNTOS PELO TRATAMENTO NO ÂMBITO DO PORTAL DO CERTIFICADO DIGITAL COVID DA UE NO QUE RESPEITA AO INTERCÂMBIO DE LISTAS DE REVOGAÇÃO DE EUDCC**

PONTO 1

*Subponto 1*

***Repartição de responsabilidades***

1) Os responsáveis conjuntos procedem ao tratamento de dados pessoais por intermédio do portal do regime de confiança, em conformidade com as especificações técnicas previstas no anexo I.

2) As autoridades emitentes dos Estados-Membros continuam a ser os únicos responsáveis pela recolha, utilização, divulgação e qualquer outro tratamento de informações sobre a revogação fora do portal, incluindo no que se refere ao procedimento conducente à revogação de um certificado.

3) Cada responsável pelo tratamento é responsável pelo tratamento de dados pessoais no portal do regime de confiança em conformidade com os artigos 5.º, 24.° e 26.° do Regulamento Geral sobre a Proteção de Dados.

4) Cada responsável pelo tratamento cria um ponto de contacto com uma caixa de correio funcional que servirá para a comunicação entre os próprios responsáveis conjuntos pelo tratamento e entre os responsáveis conjuntos pelo tratamento e o subcontratante.

5) Um grupo de trabalho criado pelo comité a que se refere o artigo 14.º do Regulamento (UE) 2021/953 será mandatado para decidir sobre quaisquer questões decorrentes do intercâmbio de listas de revogação e da responsabilidade conjunta pelo tratamento conexo de dados pessoais e para facultar instruções coordenadas à Comissão enquanto subcontratante; O processo de tomada de decisões dos responsáveis conjuntos pelo tratamento é conduzido pelo referido grupo de trabalho, de acordo com o regulamento interno por ele adotado. Como regra de base, a não participação de um dos responsáveis conjuntos pelo tratamento numa reunião deste grupo de trabalho que tenha sido anunciada, pelo menos, sete (7) dias antes da convocatória por escrito será entendida como um acordo tácito com os resultados dessa reunião. Qualquer responsável conjunto pelo tratamento pode convocar uma reunião deste grupo de trabalho.

6) As instruções são enviadas ao subcontratante por qualquer um dos pontos de contacto dos responsáveis conjuntos pelo tratamento, com o acordo dos outros responsáveis conjuntos pelo tratamento, no âmbito do processo de tomada de decisões do grupo referido na alínea 5). Esse responsável conjunto pelo tratamento envia as instruções ao subcontratante por escrito e informa desse facto os restantes responsáveis conjuntos pelo tratamento. Se a questão em apreço se revestir de tal urgência que não haja tempo para realizar uma reunião do grupo de trabalho, tal como referido na alínea 5), podem, ainda assim, ser dadas instruções, mas estas podem ser revogadas pelo grupo de trabalho. O responsável conjunto pelo tratamento em causa envia estas instruções por escrito e informa do facto, na mesma data, todos os outros responsáveis conjuntos pelo tratamento.

7) O grupo de trabalho criado nos termos da alínea 5) não exclui a competência individual dos responsáveis conjuntos pelo tratamento para informarem as respetivas autoridades de controlo competentes em conformidade com os artigos 33.º e 24.º do Regulamento Geral sobre a Proteção de Dados. Essa notificação não exige o consentimento de outros responsáveis conjuntos pelo tratamento.

8) No âmbito do portal do regime de confiança, só pessoas autorizadas pelas autoridades nacionais ou organismos oficiais designados podem aceder aos dados pessoais trocados.

9) Cada autoridade emitente mantém um registo das atividades de tratamento sob a sua responsabilidade. A responsabilidade conjunta pode ser indicada no registo.

*Subponto 2*

***Responsabilidades e funções para tramitação de pedidos e informação dos titulares dos dados***

1) Cada responsável pelo tratamento, na qualidade de autoridade emitente, fornece às pessoas singulares cujo(s) certificado(s) tenha revogado (a seguir designadas por "titulares dos dados") informações sobre a referida revogação e o tratamento dos seus dados pessoais no portal do Certificado Digital COVID da UE para efeitos de apoio ao intercâmbio de listas de revogação, em conformidade com o artigo 14.º do Regulamento Geral sobre a Proteção de Dados, a menos que tal se revele impossível ou implique um esforço desproporcionado.

2) Cada responsável pelo tratamento atua como ponto de contacto para as pessoas singulares cujo(s) certificado(s) tenha revogado e trata os pedidos apresentados por titulares de dados ou representantes dos mesmos no exercício dos direitos que lhes são conferidos pelo Regulamento Geral sobre a Proteção de Dados. Se um responsável conjunto pelo tratamento receber um pedido de um titular de dados relacionado com um certificado emitido por outro responsável conjunto pelo tratamento, informa o titular dos dados da identidade e dos contactos dessoutro responsável conjunto pelo tratamento. Se tal for solicitado por outro responsável conjunto, os responsáveis conjuntos pelo tratamento de dados prestam-se assistência recíproca na tramitação dos pedidos dos titulares dos dados e respondem uns aos outros sem atrasos indevidos e o mais tardar no prazo de um mês a contar da receção de um pedido de assistência. No caso de pedidos relacionados com dados enviados por países terceiros, o responsável pelo tratamento que recebe o pedido trata-o e informa o titular dos dados da identidade e dos contactos da autoridade emitente do país terceiro.

3) Cada responsável pelo tratamento disponibiliza aos titulares dos dados o conteúdo do presente anexo, incluindo as disposições previstas nos pontos 1 e 2.

PONTO 2

**Gestão de incidentes de segurança, incluindo violações de dados pessoais**

1) Os responsáveis conjuntos pelo tratamento assistem-se reciprocamente na identificação e no tratamento de quaisquer incidentes de segurança, incluindo violações de dados pessoais, ligados ao tratamento no portal do Certificado Digital COVID da UE.

2) Em particular, os responsáveis conjuntos pelo tratamento notificam-se mutuamente do seguinte:

   a) quaisquer riscos potenciais ou reais para a disponibilidade, confidencialidade e/ou integridade dos dados pessoais em fase de tratamento no portal do regime de confiança;

   b) qualquer violação de dados pessoais, as consequências prováveis da violação de dados pessoais e a avaliação do risco para os direitos e as liberdades de pessoas singulares, e eventuais medidas adotadas para combater a violação de dados pessoais e atenuar o risco para os direitos e as liberdades de pessoas singulares;

   c) qualquer violação de salvaguardas técnicas e/ou organizativas das operações de tratamento no portal do regime de confiança.

3) Os responsáveis conjuntos pelo tratamento comunicam eventuais violações de dados relacionadas com operações de tratamento no portal do regime de confiança à Comissão, às autoridades de controlo competentes e, se assim for requerido, aos titulares dos dados, em conformidade com os artigos 33.º e 34.º do Regulamento Geral sobre a Proteção de Dados ou após notificação pela Comissão.

4) Cada autoridade emitente aplica medidas técnicas e organizativas adequadas, a fim de:

   a) assegurar e proteger a segurança, a integridade e a confidencialidade dos dados pessoais tratados conjuntamente;

   b) proteger todos os dados pessoais na sua posse contra qualquer tratamento, perda, utilização, divulgação, aquisição ou acesso não autorizados ou ilegais;

   c) assegurar que o acesso aos dados pessoais não seja divulgado ou autorizado a outra pessoa além dos destinatários ou subcontratantes.

PONTO 3

***Avaliação de impacto sobre a proteção de dados***

1) Caso um responsável pelo tratamento precise de informações de outro responsável pelo tratamento para cumprir as obrigações especificadas nos artigos 35.º e 36.º do Regulamento (UE) 2016/679, envia um pedido específico para a caixa de correio funcional referida no ponto 1, subponto 1, alínea 4). Este último envida todos os esforços para prestar as informações solicitadas.»

*ANEXO IV*

«*ANEXO VII*

**RESPONSABILIDADES DA COMISSÃO ENQUANTO SUBCONTRATANTE NO ÂMBITO DO PORTAL DO CERTIFICADO DIGITAL COVID DA UE NO QUE RESPEITA AO APOIO AO INTERCÂMBIO DE LISTAS DE REVOGAÇÃO DE EUDCC**

A Comissão:

1) Cria e mantém em nome dos Estados-Membros uma infraestrutura de comunicação segura e fiável que apoie o intercâmbio de listas de revogação enviadas para o portal do Certificado Digital COVID.

2) Pode, para cumprir as suas obrigações enquanto subcontratante dos Estados-Membros para o portal do regime de confiança, contratar terceiros como subcontratantes ulteriores. Neste contexto, informa os responsáveis conjuntos pelo tratamento de quaisquer alterações previstas relativas ao aditamento ou substituição de outros subcontratantes, dando assim aos responsáveis pelo tratamento a oportunidade de se oporem conjuntamente a tais alterações. Assegura ainda que esses subcontratantes cumpram as mesmas obrigações em matéria de proteção de dados estabelecidas na presente decisão.

3) Procede ao tratamento dos dados pessoais apenas com base em instruções documentadas por parte dos responsáveis pelo tratamento, exceto ordem contrária nos termos do direito da União ou dos Estados-Membros. Nesse caso, a Comissão informa os responsáveis conjuntos pelo tratamento desse requisito jurídico antes de realizar a operação de tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público.

   Efetua um tratamento que implica o seguinte:

   a) autenticação de servidores de suporte nacionais, com base em certificados de servidores de suporte nacionais;

   b) receção dos dados a que se refere o artigo 5.º-A, n.º 3, da decisão carregados pelos servidores de suporte nacionais, mediante disponibilização de uma interface de programação de aplicações que permita aos referidos servidores carregar os dados pertinentes;

   c) conservação dos dados no portal do Certificado Digital COVID da UE;

   d) disponibilização dos dados para descarregamento pelos servidores de suporte nacionais;

   e) eliminação dos dados na respetiva data de expiração ou mediante instrução do responsável pelo tratamento que os tenha enviado;

   f) após o termo da prestação do serviço, eliminação de quaisquer dados remanescentes, exceto se o direito da União ou dos Estados-Membros exigir o armazenamento de dados pessoais.

4) Aplica todas as medidas de segurança mais avançadas ao nível organizacional, físico e lógico para manter o portal do Certificado Digital COVID da UE. Para esse efeito, a Comissão:

   a) designa uma entidade responsável pela gestão da segurança ao nível do portal do Certificado Digital COVID da UE, comunica aos responsáveis conjuntos pelo tratamento os dados de contacto daquela e assegura a disponibilidade da mesma para reagir a ameaças à segurança;

   b) assume a responsabilidade pela segurança do portal do Certificado Digital COVID da UE, incluindo a realização regular de testes, avaliações e análises das medidas de segurança;

   c) assegura que todas as pessoas a quem é concedido acesso ao portal do Certificado Digital COVID da UE estão sujeitas a obrigações contratuais, profissionais ou legais de confidencialidade.

5) Toma todas as medidas de segurança necessárias para evitar comprometer o bom funcionamento dos servidores de suporte nacionais. Para esse efeito, a Comissão aplica procedimentos específicos relacionados com a ligação dos servidores de suporte ao portal do Certificado Digital COVID da UE. Tal inclui:

   a) seguir um procedimento de avaliação dos riscos, a fim de identificar e estimar as potenciais ameaças ao sistema;

   b) aplicar um procedimento de auditoria e revisão para:

      i) verificar a correspondência entre as medidas de segurança postas em prática e a política de segurança aplicável,

      ii) controlar regularmente a integridade dos ficheiros de sistema, dos parâmetros de segurança e das autorizações concedidas,

iii) realizar um acompanhamento que permita detetar violações da segurança e intrusões;

iv) introduzir alterações para evitar vulnerabilidades de segurança existentes,

v) definir as condições de autorização, incluindo a pedido dos responsáveis pelo tratamento, e contribuição para a realização de auditorias independentes, incluindo inspeções, e revisões de medidas de segurança, sob reserva de condições que respeitem o Protocolo (n.º 7) do TFUE relativo aos Privilégios e Imunidades da União Europeia;

c) alterar o procedimento de controlo para documentar e medir o impacto das alterações antes da sua introdução, mantendo os responsáveis conjuntos pelo tratamento informados de quaisquer alterações que possam afetar a comunicação com as suas infraestruturas e/ou a segurança das mesmas;

d) estabelecer um procedimento de manutenção e reparação que especifique as regras e condições a seguir caso seja necessária a manutenção e/ou reparação de equipamentos;

e) estabelecer um procedimento para incidentes de segurança com vista a definir o sistema de notificação e escalada de incidentes, informar sem demora os responsáveis pelo tratamento afetados, inclusive para que estes notifiquem as autoridades nacionais de proteção de dados, sobre qualquer violação de dados pessoais, e definir um processo disciplinar para lidar com essas violações.

6) Toma medidas de segurança física e/ou lógica de ponta para as instalações que alojam o equipamento do portal do Certificado Digital COVID da UE e os controlos de acesso aos dados lógicos e à segurança. Para esse efeito, a Comissão:

a) aplica meios de segurança física para estabelecer perímetros de segurança demarcados e permitir a deteção de violações;

b) controla o acesso às instalações e mantém um registo de visitantes para fins de rastreio;

c) assegura que as pessoas externas a quem é concedido acesso às instalações são escoltadas por pessoal devidamente autorizado;

d) impede a adição, substituição ou remoção de equipamentos sem a autorização prévia dos organismos competentes designados,

e) controla o acesso recíproco entre os servidores de suporte e o portal do regime de confiança;

f) garante que as pessoas que têm acesso ao portal do Certificado Digital COVID da UE são identificadas e autenticadas;

g) revê os direitos de autorização relacionados com o acesso ao portal do Certificado Digital COVID da UE em caso de violação da segurança que afete esta infraestrutura;

h) mantém a integridade das informações transmitidas por intermédio do portal do Certificado Digital COVID da UE;

i) aplica medidas de segurança técnicas e organizativas para impedir o acesso não autorizado a dados pessoais;

j) aplica, sempre que necessário, medidas para bloquear o acesso não autorizado ao portal do Certificado Digital COVID da UE a partir do domínio das autoridades emitentes (ou seja, bloqueio de localização/endereço IP).

7) Toma medidas para proteger o seu domínio, incluindo o corte de ligações, em caso de desvio substancial em relação aos princípios e conceitos de qualidade ou segurança.

8) Mantém um plano de gestão dos riscos relacionado com a sua área de responsabilidade.

9) Acompanha — em tempo real — o desempenho de todas as componentes dos serviços do portal do regime de confiança, elabora estatísticas regulares e mantém registos.

10) Presta apoio 24 horas por dia a todos os serviços do portal do regime de confiança, em inglês, através do telefone, do correio ou do portal Web, e aceita chamadas de utilizadores autorizados: coordenadores do portal do Certificado Digital COVID da UE e respetivos serviços de assistência, responsáveis de projeto e pessoas designadas pela Comissão.

11) Assiste os responsáveis conjuntos pelo tratamento por via de medidas técnicas e organizativas adequadas, conquanto seja possível nos termos do artigo 12.º do Regulamento (UE) 2018/1725, para o cumprimento da obrigação do responsável pelo tratamento de responder aos pedidos de exercício dos direitos dos titular de dados estabelecidos no capítulo III do Regulamento Geral sobre a Proteção de Dados.

12) Apoia os responsáveis conjuntos pelo tratamento ao prestar informações sobre o portal do Certificado Digital COVID da UE, cumprindo assim as obrigações decorrentes dos artigos 32.º, 33.º, 34.º, 35.º e 36.º do Regulamento Geral sobre a Proteção de Dados.

13) Assegura que os dados tratados no âmbito do portal do Certificado Digital COVID da UE são ininteligíveis para qualquer pessoa que não esteja autorizada a aceder a esse portal.

14) Toma todas as medidas necessárias para impedir que os operadores do portal do Certificado Digital COVID da UE tenham acesso não autorizado aos dados transferidos.

15) Toma medidas para facilitar a interoperabilidade e a comunicação entre os responsáveis pelo tratamento designados do portal do Certificado Digital COVID da UE.

16) Mantém um registo das atividades de tratamento realizadas em nome dos responsáveis conjuntos pelo tratamento em conformidade com o disposto no artigo 31.º, n.º 2, do Regulamento (UE) 2018/1725.»