Jornal Oficial
da União Europeia

PT
Série L

2026/1436

12.11.2026

REGULAMENTO DELEGADO (UE) 2026/1436 DA COMISSÃO

de 1 de julho de 2026

que complementa a Diretiva (UE) 2024/2841 do Parlamento Europeu e do Conselho no respeitante à definição do código QR na versão física do cartão europeu de deficiência e à definição do código QR e de especificações técnicas comuns que garantam a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência, bem como a questões relativas à interoperabilidade

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta a Diretiva (UE) 2024/2841 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, que cria o cartão europeu de deficiência e o cartão europeu de estacionamento para pessoas com deficiência ([1]), nomeadamente o artigo 7.º, n.º 7, e o artigo 8.º, n.º 7,

Considerando o seguinte:

(1) A Diretiva (UE) 2024/2841 estabelece as regras que regem a emissão do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, bem como modelos comuns para esses cartões. Em conformidade com o artigo 7.º, n.º 2, e o artigo 8.º, n.º 2, da Diretiva (UE) 2024/2841, os cartões europeus de deficiência e os cartões europeus de estacionamento para pessoas com deficiência emitidos pelos Estados-Membros são mutuamente reconhecidos em todos os Estados-Membros.

(2) As competências previstas no artigo 7.º, n.º 7, e no artigo 8.º, n.º 7, da Diretiva (UE) 2024/2841 prosseguem o mesmo objetivo, a saber, prevenir e combater a fraude, garantir a segurança das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, nomeadamente através de medidas de segurança adequadas para os dados pessoais, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]), bem como assegurar a interoperabilidade. Atendendo a que o objeto e os objetivos das competências coincidem em grande medida, é conveniente estabelecer regras que complementem a Diretiva (UE) 2024/2841 no que diz respeito a essas matérias num único ato delegado.

(3) A Diretiva (UE) 2024/2841 prevê que as versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência contenham um código QR, funcionalidade digital de ponta que utiliza meios eletrónicos, a fim de prevenir e combater a fraude. Os códigos QR são, a este título, uma funcionalidade digital obrigatória a imprimir em todos os cartões físicos. A fim de assegurar uma abordagem uniforme na criação e utilização dos códigos QR pelos Estados-Membros, a Comissão deve adotar especificações técnicas para definir os códigos QR, nomeadamente o seu conteúdo.

(4) O cartão europeu de estacionamento para pessoas com deficiência substituirá todos os cartões de estacionamento existentes para pessoas com deficiência emitidos em conformidade com a Recomendação 98/376/CE do Conselho ([3]). Esta recomendação não foi atualizada de modo a refletir a evolução tecnológica e da digitalização, pelo que os Estados-Membros se depararam com problemas de fraude e falsificação. É, pois, necessário definir as características que garantem a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência e que têm em conta as suas especificidades, como o facto de estar geralmente colocado atrás do para-brisas do veículo.

([1]) JO L, 2024/2841, 14.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2841/oj.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Recomendação 98/376/CE do Conselho, de 4 de junho de 1998, relativa a um cartão de estacionamento para pessoas com deficiência (JO L 167 de 12.6.1998, p. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Devem ser introduzidas especificações técnicas comuns obrigatórias para garantir a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência. A impressão do cartão num material adequado, como o policarbonato, utilizando um elemento ótico difrativo variável, protegeria eficazmente contra a reprodução fraudulenta e a falsificação. Os motivos antidigitalização reforçariam ainda mais a segurança, ao permitirem detetar a duplicação do cartão, uma vez que devem conter um texto ou um motivo oculto, que deve aparecer sempre que o cartão for fotocopiado ou digitalizado. Essas características devem ser aplicadas sem afetar o formato da versão física do cartão europeu de estacionamento para pessoas com deficiência constante do anexo II da Diretiva (UE) 2024/2841, incluindo a aparência visual do cartão.

(6) Para além do código QR e de outras especificações técnicas obrigatórias definidas pelo presente regulamento, os Estados-Membros deverão ter a possibilidade de incorporar elementos de segurança digitais ou físicos facultativos, com base nas especificações técnicas comuns estabelecidas no presente regulamento, na versão física do cartão europeu de estacionamento para pessoas com deficiência, a fim de reforçar a sua segurança. Sempre que as funcionalidades digitais facultativas contenham mais dados pessoais do que os previstos nas versões físicas dos cartões, em conformidade com o anexo II, ponto 3, alínea b), da Diretiva (UE) 2024/2841, o acesso a esses dados deve ser limitado às autoridades públicas dos Estados-Membros emissores e apenas aos utilizadores autorizados. A fim de manter um quadro harmonizado para os elementos de segurança em todos os Estados-Membros, a lista de elementos facultativos deve ser exaustiva. Além disso, os Estados-Membros devem assegurar que a integração de um ou mais elementos de segurança digitais ou físicos facultativos não afete o reconhecimento de cartões válidos de outros Estados-Membros nem comprometa a interoperabilidade e a funcionalidade das especificações técnicas obrigatórias.

(7) A versão física do cartão europeu de estacionamento para pessoas com deficiência pode conter um chip de identificação por radiofrequência (RFID) como elemento de segurança digital facultativo. O RFID utiliza ondas eletromagnéticas radiantes ou um acoplamento por campo reativo na região das radiofrequências do espetro para comunicação num ou no outro sentido com uma etiqueta através de diversos sistemas de modulação e codificação, para leitura inequívoca da identidade de uma radioetiqueta ou de outros dados nela armazenados ([4]). Os chips RFID podem reforçar a proteção contra a falsificação e a manipulação através do armazenamento ou da transmissão seguros de dados relacionados com cartões. A versão física do cartão europeu de estacionamento para pessoas com deficiência pode também conter tinta oticamente variável ou tinta de variação ótica. Essas tintas proporcionam uma proteção adequada contra a cópia e a manipulação do cartão sem requererem personalização. Para garantir que os dados do cartão estão devidamente protegidos contra tentativas de contrafação e falsificação, o texto dos campos de dados pode ser integrado no material de base do cartão através da tecnologia de gravação a *laser*. Os elementos de segurança física, definidos no presente regulamento como obrigatórios ou facultativos, que não sejam visíveis ou que se tornem visíveis na sequência de determinadas manipulações, não estão em contradição com o formato do cartão europeu de estacionamento para pessoas com deficiência estabelecido no anexo II da Diretiva (UE) 2024/2841.

(8) Os avanços tecnológicos, os sistemas de verificação do estacionamento e os riscos de segurança estão em constante evolução. O estado da técnica está em constante desenvolvimento e a utilização do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência evolui, impulsionada tanto pelas reações dos utilizadores como pelo progresso tecnológico, tal como as técnicas de fraude e falsificação, o que conduz à evolução dos desafios de segurança. Assim, as novas soluções tecnológicas, incluindo as relacionadas com a verificação do estacionamento, bem como as necessidades de segurança e de prevenção antifraude, podem exigir alterações na arquitetura de segurança e antifraude dos cartões, nomeadamente através da atualização da categorização das funcionalidades digitais como obrigatórias ou facultativas. Em função da evolução tecnológica, a atualização do presente regulamento poderá ser necessária.

(9) A fim de assegurar que as versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência possam ser utilizadas sem interrupções em todos os Estados-Membros, é imprescindível garantir a interoperabilidade das funcionalidades digitais nos cartões físicos, em especial dos códigos QR. A interoperabilidade deverá permitir a verificação da autenticidade e da validade das versões físicas dos cartões pelos verificadores de cartões — ou seja, por qualquer pessoa singular ou coletiva que verifique a validade e a autenticidade das versões físicas dos cartões, por exemplo, através de uma aplicação de verificação. Para este efeito, é necessário estabelecer disposições sobre questões relacionadas com a interoperabilidade, de modo a permitir verificações transfronteiras das versões físicas dos cartões de forma coerente e fiável.

([4]) Recomendação 2009/387/CE da Comissão, de 12 de maio de 2009, relativa à aplicação dos princípios de proteção da privacidade e dos dados nas aplicações assentes na identificação por radiofrequências (JO L 122 de 16.5.2009, p. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) A fim de assegurar a integridade e a origem dos dados contidos nos códigos QR nas versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, esses dados devem ser selados com um selo eletrónico qualificado, na aceção do artigo 3.º, ponto 27, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([5]). O código QR confirma a autenticidade e a validade do cartão físico, quando cruzado com os parâmetros de verificação, e não pode, por si só, atestar o estatuto de deficiência ou o direito a serviços específicos em razão de uma deficiência.

(11) No intuito de facilitar a interoperabilidade e a criação de um sistema de verificação fiável e seguro das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência em toda a União, devem ser criados mecanismos de notificação e publicação de informações. A este respeito, e a fim de permitir a verificação de que as versões físicas dos cartões são emitidas por uma autoridade ou um organismo competente, os Estados-Membros devem fornecer as informações necessárias para o processo de verificação, mais concretamente as informações necessárias para verificar o selo eletrónico qualificado. Os Estados-Membros devem, pois, ser obrigados a notificar à Comissão as autoridades ou organismos competentes responsáveis pela emissão das versões físicas dos cartões (emitentes de cartões), bem como as informações administrativas e técnicas pertinentes que lhes digam respeito. As informações a notificar à Comissão devem limitar-se ao necessário para a criação de mecanismos de verificação interoperáveis que possam verificar a validade e a autenticidade das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência. Cabe à Comissão assegurar o acesso do público a essas informações.

(12) Além disso, em caso de revogação do cartão, devem ser prontamente disponibilizadas informações sobre essa revogação, a fim de permitir que os verificadores verifiquem a validade do cartão. Para este efeito, os emitentes de cartões devem manter e publicar atempadamente listas que contenham informações sobre o estado de revogação de todos os cartões que tenham revogado antes do termo das respetivas datas de expiração (listas de revogação). Essa publicação deve respeitar a privacidade e proteger os dados pessoais dos titulares dos cartões. Além disso, as listas de revogação não podem conter quaisquer dados pessoais para além dos identificadores únicos de revogação e devem ser publicadas num identificador uniforme de recurso (URI) específico, em conformidade com as especificações técnicas, a fim de assegurar uma verificação interoperável.

(13) Para ler o código QR e verificar a autenticidade e a validade das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, a nível nacional, podem ser utilizadas aplicações de verificação personalizadas. A Comissão pode apoiar este processo fornecendo uma amostra comum de código-fonte para a leitura dos dados contidos nos códigos QR e para a realização das principais etapas do processo de verificação, que podem servir de base para as aplicações de verificação nos Estados-Membros. Todas as aplicações de verificação devem executar a mesma lógica de verificação da cadeia de confiança com a mesma infraestrutura de confiança, permitindo, assim, a leitura dos dados codificados nos cartões pelo Estado-Membro emissor. Além disso, o anexo I da Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho ([6]) estabelece requisitos de acessibilidade que os Estados-Membros devem cumprir, quando aplicável.

(14) Ao reconhecer a natureza dinâmica dos avanços tecnológicos e a evolução das ameaças à cibersegurança, a União mostra o seu empenho em assegurar que os mecanismos criptográficos utilizados no âmbito do seu quadro normativo continuem a ser eficazes e seguros. À luz deste compromisso, é importante proceder à adoção de normas criptográficas aprovadas pelo Grupo Europeu para a Certificação da Cibersegurança e divulgadas através da Agência da União Europeia para a Cibersegurança (ENISA).

(15) O Regulamento (UE) 2016/679 é aplicável ao tratamento de dados pessoais efetuado ao abrigo do presente regulamento. Em especial, a verificação dos códigos QR nas versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência implica o tratamento de dados pessoais. Assim, devem ser estabelecidas garantias adequadas em matéria de proteção de dados para assegurar a proteção dos dados pessoais contidos nos códigos QR, em conformidade com o Regulamento (UE) 2016/679, se aplicável. As medidas gerais de segurança previstas no presente regulamento devem também assegurar a proteção dos dados pessoais contidos nos códigos QR. Além disso, os dados pessoais contidos nos códigos QR devem limitar-se ao estritamente necessário para efeitos do presente regulamento. Mais ainda, deve ser proibida a conservação dos dados após a verificação ter sido concluída. É igualmente indispensável garantir segurança adequada para as listas de revogação.

([5]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos requisitos de acessibilidade dos produtos e serviços (JO L 151 de 7.6.2019, p. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) Em conformidade com o artigo 14.º, n.º 4, da Diretiva (UE) 2024/2841, para a elaboração do presente regulamento, a Comissão consultou as pessoas com deficiência e as organizações que as representam, bem como os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([7]).

(17) O cartão europeu de deficiência e o cartão europeu de estacionamento para pessoas com deficiência constituem um serviço público digital transeuropeu, na aceção do Regulamento (UE) 2024/903 do Parlamento Europeu e do Conselho ([8]). Foi, pois, realizada uma avaliação da interoperabilidade e o relatório resultante deve ser publicado no portal Europa Interoperável a que se refere o artigo 8.º do Regulamento (UE) 2024/903.

(18) A Autoridade Europeia para a Proteção de Dados foi consultada sobre o presente regulamento em conformidade com o artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([9]) e emitiu parecer em 12 de maio de 2026,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto e âmbito de aplicação

O presente regulamento estabelece as regras que complementam a Diretiva (UE) 2024/2841 no que se refere aos seguintes aspetos:

a) Definição do código QR para as versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, incluindo medidas de segurança adequadas para os dados pessoais;

b) Definição de especificações técnicas comuns obrigatórias e facultativas que garantam a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência;

c) Definição dos requisitos de interoperabilidade necessários para assegurar que os códigos QR nas versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência emitidos num Estado-Membro possam ser lidos e verificados de forma fiável noutro Estado-Membro.

Artigo 2.º

Código QR na versão física do cartão europeu de deficiência

As especificações do código QR que deve figurar na versão física do cartão europeu de deficiência são as definidas no anexo I.

Artigo 3.º

Código QR na versão física do cartão europeu de estacionamento para pessoas com deficiência

As especificações do código QR que deve figurar na versão física do cartão europeu de estacionamento para pessoas com deficiência são as definidas no anexo II.

([7]) JO L 123 de 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([8]) Regulamento (UE) 2024/903 do Parlamento Europeu e do Conselho, de 13 de março de 2024, que estabelece medidas para um elevado nível de interoperabilidade do setor público em toda a União (Regulamento Europa Interoperável) (JO L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artigo 4.º

Especificações técnicas comuns obrigatórias para o cartão europeu de estacionamento para pessoas com deficiência

1. As versões físicas do cartão europeu de estacionamento para pessoas com deficiência devem cumprir as seguintes especificações técnicas comuns:

(a) Devem ser feitas de um material que proteja contra a delaminação e seja capaz de cumprir os requisitos definidos no anexo II da Diretiva (UE) 2024/2841, assim como outras especificações técnicas comuns obrigatórias definidas no presente artigo;

(b) Devem conter um elemento ótico difrativo variável sob a forma de um elemento de estrutura em camadas que se torna visível quando o cartão é visto de um determinado ângulo;

(c) Devem ser dotados de um motivo antidigitalização que se torna visível quando um cartão é fotocopiado ou digitalizado.

2. O elemento ótico difrativo variável a que se refere o n.º 1, alínea b), deve figurar na parte da frente da versão física do cartão europeu de estacionamento para pessoas com deficiência, num ou mais campos de dados do lado esquerdo. Deve ter aproximadamente 20 mm de altura e 20 mm de largura. A imagem apresentada no dispositivo consiste num mapa estilizado ou no código distintivo do Estado-Membro emissor rodeado por um círculo de 12 estrelas que simboliza a União.

3. O motivo antidigitalização a que se refere o n.º 1, alínea c), deve estar na parte da frente da versão física do cartão europeu de estacionamento para pessoas com deficiência, acima dos campos de dados do lado esquerdo e/ou do lado direito, fora do código QR e da sua zona em branco. Deve conter um texto ou um motivo oculto, que deve aparecer sempre que o cartão for fotocopiado ou digitalizado. Se o motivo antidigitalização contiver um texto oculto, deve ser constituído pelas palavras «COPY» (CÓPIA) ou «VOID» (SEM EFEITO) e pela correspondente tradução numa ou mais línguas oficiais do Estado-Membro emissor. Se o motivo antidigitalização contiver um padrão oculto, este deve ser composto por linhas horizontais ou verticais.

Artigo 5.º

Especificações e características técnicas facultativas para a segurança do cartão europeu de estacionamento para pessoas com deficiência

1. Para além das especificações técnicas comuns obrigatórias a que se refere o artigo 4.º, os Estados-Membros só podem aplicar as especificações técnicas e características facultativas definidas no presente artigo.

2. As versões físicas do cartão europeu de estacionamento para pessoas com deficiência podem conter um chip de identificação por radiofrequência (RFID). O chip RFID deve prevenir e combater a fraude através de meios eletrónicos e servir de meio adicional de verificação da autenticidade e/ou da validade, a nível nacional, de uma versão física do cartão europeu de estacionamento para pessoas com deficiência. O chip RFID não pode afetar o funcionamento do código QR no cartão.

3. Qualquer chip RFID referido no n.º 2 deve cumprir as seguintes especificações:

a) Deve ser passivo;

b) Deve estar fisicamente integrado no corpo do cartão da parte da frente, no lado direito;

c) Deve estar ligado, de forma lógica, ao registo do código QR e conter o mesmo identificador de revogação (RID) do que o codificado no código QR;

d) A funcionalidade RFID deve suportar leituras a cerca de um metro ou mais, quando exigido para utilização operacional, mas não deve ser concebida para leituras fiáveis a distâncias superiores a cinco metros em condições de ensaio de referência;

e) Após a emissão do cartão, o acesso para escrita ao chip RFID, ou à zona de dados pertinente do mesmo, deve ser impedido ou controlado de outra forma pela autoridade emissora;

f) Deve ser concebido e configurado de modo a minimizar o risco de clonagem, substituição, modificação não autorizada e reescrita não autorizada;

g) Deve cumprir os requisitos da Diretiva 2014/53/UE do Parlamento Europeu e do Conselho ([10]);

h) Para além do RID a que se refere a alínea c), o chip RFID pode memorizar apenas um ou mais dos seguintes elementos:

i) dados codificados no código QR da versão física do cartão europeu de estacionamento para pessoas com deficiência,

ii) número(s) de matrícula do veículo,

iii) dados de verificação criptográfica.

4. A parte da frente das versões físicas do cartão europeu de estacionamento para pessoas com deficiência pode conter uma ou mais das seguintes características:

a) O símbolo da cadeira de rodas no lado esquerdo ou a menção «cartão europeu de estacionamento para pessoas com deficiência» em inglês e numa ou mais línguas oficiais do Estado-Membro emissor no lado direito, impressa com tinta oticamente variável ou tinta de variação ótica e que, quando visto a partir de diferentes ângulos, revele cores que podem variar;

b) Utilização da tecnologia de gravação a *laser* que penetra nas camadas do cartão para imprimir o texto nos campos de dados.

5. A introdução das especificações e características técnicas facultativas a que se refere o presente artigo não afeta o reconhecimento, no Estado-Membro que introduziu essas características para os cartões que emite, dos cartões válidos emitidos noutros Estados-Membros.

Artigo 6.º

Questões relativas à interoperabilidade

1. As informações incluídas no código QR devem ser seladas com um selo eletrónico qualificado na aceção do artigo 3.º, ponto 27, do Regulamento (UE) n.º 910/2014.

2. Cabe a cada Estado-Membro comunicar à Comissão informações sobre as autoridades ou organismos competentes responsáveis pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência («emitentes de cartões»), bem como quaisquer atualizações subsequentes dessas informações, em conformidade com o anexo III. Cabe à Comissão assegurar o acesso do público a essas informações.

3. Os emitentes de cartões devem manter e publicar, num identificador uniforme de recurso notificado à Comissão, listas de revogação atualizadas que contenham informações sobre o estado de revogação de todos os cartões que tenham revogado em conformidade com as especificações técnicas definidas no anexo IV. As informações sobre a revogação devem ser publicadas no prazo de 24 horas a contar dessa revogação.

4. Os Estados-Membros podem utilizar aplicações de verificação para verificar a autenticidade e a validade das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência.

5. Sempre que os Estados-Membros utilizem aplicações de verificação para verificar a autenticidade e a validade das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência, essas aplicações devem permitir verificar a autenticidade e a validade de um cartão, através da verificação do selo eletrónico e do estado de revogação do cartão. Estas aplicações de verificação devem apresentar e poder ler uma representação visual dos dados pessoais codificados no código QR do cartão, conforme estabelecido nos anexos I e II, a fim de permitir uma comparação com os dados visíveis nos campos de dados correspondentes no cartão, bem como uma indicação relativa à validade do cartão.

([10]) Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Artigo 7.º

Medidas de segurança para a proteção dos dados pessoais

1. Os dados pessoais contidos nos códigos QR nas versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência devem limitar-se ao estritamente necessário para verificar a autenticidade e a validade dos cartões, conforme estabelecido nos anexos I e II.

2. Após a conclusão da verificação da autenticidade e validade de uma versão física do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência pelos verificadores de cartões, os dados contidos nos códigos QR não podem ser conservados pelos verificadores de cartões.

3. A verificação de um código QR numa versão física do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência não pode dar lugar à notificação dessa verificação à autoridade ou organismo competente responsável pela emissão do cartão.

4. As informações incluídas numa lista de revogação publicada em conformidade com o artigo 6.º, n.º 3, devem limitar-se ao identificador de revogação dos cartões revogados.

5. A autoridade ou o organismo responsável pela publicação das listas de revogação nos termos do artigo 6.º, n.º 3, deve assegurar a aplicação de medidas de segurança técnicas e organizativas adequadas ao tratamento dos dados pessoais constantes das listas de revogação.

6. Sempre que um Estado-Membro decida incorporar um chip RFID na versão física do cartão europeu de estacionamento para pessoas com deficiência, os n.ºs 2 a 3 são aplicáveis ao tratamento dos dados pessoais contidos nesse chip. Os dados pessoais contidos no chip RFID devem limitar-se ao estritamente necessário para verificar a autenticidade e/ /ou validade dos cartões, conforme estabelecido no artigo 5.º, n.º 3.

Sempre que um Estado-Membro armazene no chip RFID dados pessoais a que se refere o artigo 5.º que não constem da versão física do cartão europeu de estacionamento para pessoas com deficiência, conforme estabelecido no anexo II da Diretiva (UE) 2024/2841, o acesso a esses dados deve ser limitado às autoridades públicas do Estado-Membro emissor e apenas aos utilizadores autorizados.

Artigo 8.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 1 de julho de 2026.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

ESPECIFICAÇÕES DO CÓDIGO QR PARA A VERSÃO FÍSICA DO CARTÃO EUROPEU DE DEFICIÊNCIA

1. **Formato do código QR para a versão física do cartão europeu de deficiência**

a) **Formato do código QR Modelo 2**, em conformidade com as especificações internacionais do código QR ISO/IEC 18004:2024 ou equivalentes.

b) **Nível de correção de erro M** (redundância de 15 %) que assegura a proteção contra riscos ou danos parciais de um código QR impresso.

c) **Modo de codificação**: A carga útil do QR é constituída pela estrutura combinada issuerSigned Concise Binary Object Representation (representação concisa de objetos binários) (CBOR) e pelo correspondente objeto de assinatura issuerAuth COSE_Sign1, conforme definido em CBOR Object Signing and Encryption (*assinatura e codificação de objetos*) (COSE, RFC 9052, secções 3.1, 4.2 e 4.4), segundo o padrão de modelo de dados mDOC para os elementos issuerSigned, mas adaptado para utilização estática num cartão físico. O issuerAuth deve ser um objeto COSE_Sign1 com alg = ES256 e um cabeçalho protegido que contenha um valor x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256].

d) Antes da codificação do código QR, o objeto combinado CBOR/COSE deve ser **comprimido utilizando o formato zlib** (RFC 1950, secção 2.2) **com o algoritmo deflate** (RFC 1951, secções 3.2 e 4). A matriz de bytes (byte array) comprimida resultante deve ser codificada **sob a forma de bytes para código QR**, para assegurar a total compatibilidade com cargas úteis binárias CBOR/COSE e a interoperabilidade do digitalizador.

Para todos os campos de texto incluídos na carga útil do código QR, os emitentes devem introduzir carateres com codificação Unicode UTF-8 nas cadeias de texto CBOR. A transliteração não pode ser aplicada aos dados de carga útil assinados. Para efeitos de interoperabilidade, os emitentes devem aplicar a Forma de Normalização Unicode C (NFC) a todos os campos textuais antes de assinar.

e) **Prefixo:** A cadeia de carateres do código QR para o cartão europeu de deficiência começa por «ED1: MDOC:». Isto identifica o tipo de cartão e o perfil de codificação. Os prefixos são sensíveis às maiúsculas e minúsculas e devem estar presentes. Os prefixos desconhecidos ou não suportados serão causa de rejeição. O prefixo e a carga útil comprimida devem ser codificados no código QR como um único segmento de dados sob a forma de bytes.

f) **Dimensão mínima do módulo ≥ 0,25 mm** para garantir a legibilidade nos cartões impressos.

g) **Versão 20, no máximo**; com até 97 × 97 módulos de cada lado.

2. **Especificações para gerar assinaturas para o cartão europeu de deficiência**

O selo eletrónico qualificado (QSeal) utilizado para selar os códigos QR do cartão europeu de deficiência garante que os dados codificados provêm da autoridade emissora autorizada e que não foram alterados.

a) **Algoritmo de assinatura**: O algoritmo de assinatura deve ser ES256 [algoritmo de assinatura digital de curva elíptica (ECDSA) com SHA-256 e utilizando a curva P-256], conforme definido no RFC 9053 (secção 2.1); no COSE, o algoritmo é identificado pelo parâmetro do cabeçalho «alg» no RFC 9052 (secção 3.1).

b) **Chave de assinatura**: A carga útil do código QR deve ser assinada utilizando a chave privada correspondente a um certificado qualificado de selo eletrónico (QSealC).

c) **Estrutura COSE**: O contentor da assinatura deve ser um objeto COSE_Sign1. O cabeçalho protegido deve incluir os valores alg (ES256) e x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256]. A verificação deve basear-se na utilização do valor x5t para localizar o certificado correspondente na lista de certificados de confiança armazenada na memória cache local do verificador, construída a partir de informações da Lista de Confiança e, em seguida, validar a cadeia de certificados e o estado do certificado em conformidade com o quadro de confiança eIDAS.

d) **Norma de assinatura**: A assinatura da carga útil do código QR deve ser um objeto COSE_Sign1, em conformidade com o RFC 9052 (secção 4), CBOR Object Signing and Encryption (*assinatura e codificação de objetos*). O objeto COSE_Sign1 deve ser transportado pelo issuerAuth e codificado sem a etiqueta CBOR para COSE_Sign1. O campo da carga útil do objeto COSE_Sign1 deve ser separado e codificado com um valor CBOR nulo. Para a criação e verificação da assinatura, a carga útil externa deve consistir na estrutura CBOR determinística que contém os valores docType e issuerSigned do mapa CBOR de nível superior.

e) **Algoritmo de dispersão (Hash)**: O SHA-256 deve ser utilizado como parte do ES256 para gerar assinaturas e verificação da integridade.

f) **Codificação**: A carga útil deve ser codificada utilizando o CBOR (RFC 8949, secção 4.2), conforme exigido pelas especificações COSE e mDOC, para assegurar a codificação e a reprodutibilidade dos dados assinados.

3. **Especificações de impressão:**

a) **Zona em branco**: O código QR deve ser contornado, em todos os lados, por uma margem vazia de **quatro módulos** sem qualquer impressão, padrão ou fundo.

b) **Contraste**: O código QR deve ser impresso sobre um fundo branco, com uma relação de contraste mínima de **4:1**, a fim de assegurar uma elevada legibilidade em condições de iluminação variáveis.

c) O código QR deve ser impresso utilizando a cor definida no anexo I da Diretiva (UE) 2024/2841 que garanta o máximo contraste.

d) **Colocação e dimensão**: O código QR, incluindo a zona em branco, deve ser de 26,25 mm × 26,25 mm, no verso do cartão, no canto inferior direito. O código QR deve ser, no máximo, a versão 20 (97 × 97 módulos), com um módulo de dimensão igual ou superior a 0,25 mm.

O código QR, incluindo a zona em branco, deve estar posicionado a, pelo menos, 5 mm da margem direita e a, pelo menos, 5 mm da margem inferior do cartão.

4. **Dados no código QR do cartão europeu de deficiência**

O código QR deve conter um conjunto de dados mínimo verificável fora de linha, em conformidade com o princípio da minimização dos dados consagrado pelo artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679. A estrutura da carga útil é a seguinte:

a) Os atributos do cartão são codificados no CBOR num objeto issuerSigned.

b) A estrutura é encapsulada e assinada pelo QSeal da autoridade emissora como issuerAuth (COSE_Sign1, ES256, incluindo um valor x5t, o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

c) O objeto CBOR/COSE resultante deve ser comprimido de acordo com o ponto 1, alínea d) do presente anexo. A carga útil do código QR deve consistir no prefixo «ED1:MDOC:», seguido da matriz de bytes comprimida resultante, e a carga útil completa deve ser codificada utilizando o formato binário como um único segmento de dados do código QR.

O conteúdo dos dados deve consistir num subconjunto de dados visíveis que figurem nos campos da parte da frente do cartão enumerados no anexo I da Diretiva (UE) 2024/2841 (nome, apelido, número de série do cartão, data de expiração), juntamente com o identificador de revogação, a assinatura eletrónica e as informações sobre o esquema.

A assinatura eletrónica deve conter:

i) issuerAuth — objeto COSE_Sign1 assinado com a **chave privada QSealC** da autoridade emissora.

ii) cabeçalho protegido que inclui os valores alg = ES256 (algoritmo de assinatura) e x5t (o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

5. **Dados facultativos**

Não devem ser incluídos dados facultativos no código QR.

6. **Identificador de revogação**

Para além do número de série visível do cartão, o código QR deve incluir um identificador de revogação específico.

O identificador de revogação deve ser utilizado para determinar o estado de revogação e para a gestão da lista de revogação. O identificador de revogação não pode ser impresso no cartão nem apresentado aos verificadores de cartões.

6.1. *Obrigações do identificador de revogação*

O identificador de revogação:

a) Deve ser incluído na carga útil assinada do QR;

b) Deve ser único, pelo menos, no domínio de emissão da autoridade emissora;

c) Não pode ser impresso no cartão nem destinar-se a ser compreendida por humanos;

d) Não pode revelar dados pessoais nem ter um significado diretamente identificável;

e) Não pode ser dedutível diretamente a partir do número de série visível do cartão; e

f) Deve estar criptograficamente ligado à carga útil do código QR pelo selo eletrónico qualificado.

6.2. *Formato e dimensão do identificador de revogação*

O identificador de revogação deve ser codificado como uma cadeia de bytes CBOR (bstr). O identificador de revogação deve ter um comprimento de16 bytes (128 bits).

O identificador de revogação deve ser gerado pela autoridade emissora utilizando um método sob o seu controlo que garanta entropia e resistência suficientes contra tentativas de decifração ou enumeração.

6.3. *Listas de revogação*

As listas de revogação publicadas para efeitos de verificação devem fazer referência apenas ao identificador de revogação dos cartões revogados. Os números de série dos cartões não podem ser publicados nas listas de revogação.

7. **Carga útil CBOR (dentro do código QR) do cartão europeu de deficiência**

Apenas os seguintes dados devem ser incluídos na carga útil do código QR, em consonância com os campos de dados visíveis do cartão europeu de deficiência estabelecidos no anexo I da Diretiva (UE) 2024/2841.

Conteúdos de nível superior:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" com os atributos indicados no quadro abaixo

c) issuerAuth = COSE_Sign1 (QSeal)

Campo	caminho de acesso mDOC	Tipo/Formato
Versão do esquema de dados	issuerSigned.nameSpaces."eu.edc".ver	Cadeia de carateres alfanuméricos (p. ex., "1.0")
Tipo de cartão: cartão europeu de deficiência	docType	Enum ("eu.edc")
Número de série do cartão	issuerSigned.nameSpaces."eu.edc".sub	Cadeia de carateres alfanuméricos
Identificador de revogação	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bytes)
Nome próprio do titular do cartão	issuerSigned.nameSpaces."eu.edc".givenName	Cadeia de texto Unicode (UTF-8)
Apelido do titular do cartão	issuerSigned.nameSpaces."eu.edc".familyName	Cadeia de texto Unicode (UTF-8)
Data de validade do cartão	issuerSigned.nameSpaces."eu.edc".exp	Etiqueta CBOR 1004, conforme definida no RFC 8943 (secção 2.1), que contém uma cadeia de carateres de texto com codificação UTF-8 que representa uma data completa RFC 3339 no formato AAAA-MM-DD

A assinatura eletrónica é transportada pelo issuerAuth (um objeto COSE_Sign1). A cadeia de certificados não pode ser incorporada na carga útil do código QR; em vez disso, o cabeçalho protegido COSE deve incluir um valor x5t, um código de identificação digital do certificado utilizado para localizar o QSealC correspondente na lista de certificados de confiança armazenada na memória cache do verificador.

8. **Exemplo de carga útil do código QR do cartão europeu de deficiência: representação lógica comentada no estilo de notação de objetos JavaScript**

O exemplo que se segue é uma representação do esquema lógico do cartão europeu de deficiência em notação JSON que pode ser compreendida por humanos. Na prática, esta estrutura não pode ser compreendida por humanos, uma vez que:

a) É codificada no CBOR (RFC 8949, secção 3);

b) É assinada utilizando uma estrutura COSE_Sign1 sem etiqueta com uma carga útil separada (RFC 9052, secção 4);

c) Incluirá uma etiqueta CBOR 1004 com a data de expiração no formato de valor de data completa, de acordo com o RFC 8943 (secção 2.1);

d) Incluirá o parâmetro de cabeçalho protegido x5t, em conformidade com o RFC 9360, utilizando o SHA-256 sobre o QSealC de entidade final codificado em DER; e

e) É comprimida e pré-fixada com a cadeia de carateres ED1:MDOC: antes de ser codificada no código QR.

```
{
  // Apenas esquema lógico do cartão europeu de deficiência, em formato JSON legível por humanos.
  // A carga útil real do código QR é CBOR determinístico e não JSON.
  "docType": "eu.edc", // credencial do cartão europeu de deficiência. O valor docType está incluído, juntamente com
     // issuerSigned, na carga útil externa COSE_Sign1.

  "issuerSigned": {
     // Dados protegidos por issuerAuth; utilizado como carga útil separada.
     // Para a criação e verificação da assinatura, a carga útil externa separada abrange
     // docType e issuerSigned.
     "nameSpaces": {
       "eu.edc": {
         "ver": "1.0", // perfil QR/versão do esquema

         // Número de série do cartão; definido pelo emitente, máx. 24 carateres.
         "sub": "AB123456789012345678 90CD",

         // Identificador de revogação: CBOR bstr real, 16 bytes/128 bits.
         // Apresentado aqui como 32 carateres hexadecimais para legibilidade.
         "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

         "givenName": "Ann", // nome próprio impresso no cartão europeu de deficiência
         "familyName": "Other", // apelido impresso no cartão europeu de deficiência

         // A codificação CBOR real utiliza a etiqueta 1004 para a data completa RFC 3339.
         "exp": "2030-12-31"
       }
     }
  },

  "issuerAuth": {
    // Formulário efetivo: COSE_Sign1 sem etiqueta, não um objeto JSON.
    "type": "COSE_Sign1",
```

```
"tagged": falso, // codificado sem etiqueta CBOR COSE_Sign1
"payload": "detached", // O campo da carga útil COSE é CBOR nulo.

"protectedHeader": {
  // alg: ES256; parâmetro de cabeçalho COSE equivalente 1 = -7.
  "alg": "ES256",

  // x5t: código de identificação digital do certificado; parâmetro de cabeçalho COSE 34.
  "x5t": {
    "hashAlg": "SHA-256", valor de dispersão equivalente COSE -16

    // Valor de dispersão SHA-256 do QSealC de entidade final codificado em DER.
    // 32 bytes representados por 64 carateres hexadecimais.
    "hashValue":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
  }
},

"unprotectedHeader": {}, // em branco neste exemplo

// Assinatura ES256 COSE: 64 bytes = 128 carateres hexadecimais.
"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
f0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. **Utilização de mecanismos criptográficos**

A utilização de mecanismos criptográficos no contexto do presente anexo deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA).

ANEXO II

ESPECIFICAÇÕES DO CÓDIGO QR PARA A VERSÃO FÍSICA DO CARTÃO EUROPEU DE ESTACIONAMENTO PARA PESSOAS COM DEFICIÊNCIA

1. **Formato do código QR na versão física do cartão europeu de estacionamento para pessoas com deficiência**

   a) **Formato do código QR Modelo 2**, em conformidade com as especificações internacionais do código QR ISO/IEC 18004:2024 ou equivalentes.

   b) **Nível de correção de erro M** (redundância de 15 %) que assegura a proteção contra riscos ou danos parciais de um código QR impresso.

   c) **Modo de codificação**: A carga útil do QR é constituída pela estrutura combinada issuerSigned Concise Binary Object Representation (representação concisa de objetos binários) (CBOR) e pelo correspondente objeto de assinatura issuerAuth COSE_Sign1, conforme definido em CBOR Object Signing and Encryption (*assinatura e codificação de objetos*) (COSE, RFC 9052, secções 3.1, 4.2 e 4.4), segundo o padrão de modelo de dados mDOC para os elementos issuerSigned, mas adaptado para utilização estática num cartão físico. O issuerAuth deve ser um objeto COSE_Sign1 com alg = ES256 e um cabeçalho protegido que contenha um valor x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256].

   d) Antes da codificação do código QR, o objeto combinado CBOR/COSE deve ser **comprimido utilizando o formato zlib (RFC 1950, secção 2.2) com o algoritmo deflate** (RFC 1951, secções 3.2 e 4). A matriz de bytes (byte array) comprimida resultante deve ser codificada **sob a forma de bytes para código QR**, para assegurar a total compatibilidade com cargas úteis binárias CBOR/COSE e a interoperabilidade do digitalizador.

   Para todos os campos de texto incluídos na carga útil do código QR, os emitentes devem introduzir carateres com codificação Unicode UTF-8 nas cadeias de texto CBOR. A transliteração não pode ser aplicada aos dados de carga útil assinados. Para efeitos de interoperabilidade, os emitentes devem aplicar a Forma de Normalização Unicode C (NFC) a todos os campos textuais antes de assinar.

   e) **Prefixo**: A cadeia de carateres do código QR para o cartão europeu de estacionamento para pessoas com deficiência começa por «EP1:MDOC:». Isto identifica o tipo de cartão e o perfil de codificação. Os prefixos são sensíveis às maiúsculas e minúsculas e devem estar presentes. Os prefixos desconhecidos ou não suportados serão causa de rejeição. O prefixo e a carga útil comprimida devem ser codificados no código QR como um único segmento de dados sob a forma de bytes.

   f) **Dimensão mínima do módulo ≥ 0,35 mm** para garantir a legibilidade nos cartões impressos.

   g) **Versão 20, no máximo**; com até 97 × 97 módulos de cada lado.

2. **Especificações para gerar assinaturas para o cartão europeu de estacionamento para pessoas com deficiência**

   O selo eletrónico qualificado (QSeal) utilizado para selar os códigos QR do cartão europeu de estacionamento para pessoas com deficiência garante que os dados codificados provêm da autoridade emissora autorizada e que não foram alterados.

   a) **Algoritmo de assinatura**: O algoritmo de assinatura deve ser ES256 (ECDSA com SHA-256 e utilizando a curva P-256), conforme definido no RFC 9053 (secção 2.1); no COSE, o algoritmo é identificado pelo parâmetro do cabeçalho «alg» no RFC 9052 (secção 3.1).

   b) **Chave de assinatura**: A carga útil do código QR deve ser assinada utilizando a chave privada correspondente a um certificado qualificado de selo eletrónico (QSealC).

   c) **Estrutura COSE**: O contentor da assinatura deve ser um objeto COSE_Sign1. O cabeçalho protegido deve incluir os valores alg (ES256) e x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256]. A verificação deve basear-se na utilização do valor x5t para localizar o certificado correspondente na lista de certificados de confiança armazenada na memória cache local do verificador, construída a partir de informações da Lista de Confiança e, em seguida, validar a cadeia de certificados e o estado do certificado em conformidade com o quadro de confiança eIDAS.

   d) **Norma de assinatura**: A assinatura da carga útil do código QR deve ser um objeto COSE_Sign1, em conformidade com o RFC 9052 (secção 4), CBOR Object Signing and Encryption (*assinatura e codificação de objetos*). O objeto COSE_Sign1 deve ser transportado pelo issuerAuth e codificado sem a etiqueta CBOR para COSE_Sign1. O campo da carga útil do objeto COSE_Sign1 deve ser separado e codificado com um valor CBOR nulo. Para a criação e verificação da assinatura, a carga útil externa deve consistir na estrutura CBOR determinística que contém os valores docType e issuerSigned do mapa CBOR de nível superior.

e) **Algoritmo de dispersão (Hash)**: O SHA-256 é utilizado como parte do ES256 para gerar assinaturas e verificação da integridade.

f) **Codificação**: A carga útil deve ser codificada utilizando o CBOR (RFC 8949, secção 4.2), conforme exigido pelas especificações COSE e mDOC, para assegurar a codificação e a reprodutibilidade dos dados assinados.

3. **Especificações de impressão:**

a) **Zona em branco**: O código QR deve ser contornado, em todos os lados, por uma margem vazia de **quatro módulos** sem qualquer impressão, padrão ou fundo.

b) **Contraste**: O código QR deve ser impresso sobre um fundo branco, com uma relação de contraste mínima de **4:1**, a fim de assegurar uma elevada legibilidade em condições de iluminação variáveis.

c) O código QR deve ser impresso utilizando a cor definida no anexo II da Diretiva (UE) 2024/2841 que garanta o máximo contraste.

d) **Colocação e dimensão**: O código QR, incluindo a zona em branco, deve ser de **37 mm × 37 mm**, na parte da frente do cartão, ligeiramente à direita do centro, em direção à margem inferior. O código QR deve ser, no máximo, a versão 20 (97 × 97 módulos), com um módulo de dimensão igual ou superior a 0,35 mm.

O código QR, incluindo a sua zona em branco, deve estar posicionado a, pelo menos, 5 mm da margem inferior do cartão.

4. **Dados no código QR do cartão europeu de estacionamento para pessoas com deficiência**

O código QR deve conter um conjunto de dados mínimo verificável fora de linha, em conformidade com o princípio da minimização dos dados consagrado pelo artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679. A estrutura da carga útil é a seguinte:

a) Os atributos do cartão são codificados no CBOR num objeto issuerSigned.

b) Esta estrutura é encapsulada e assinada pelo QSeal da autoridade emissora como emissorAuth (COSE_Sign1, ES256, incluindo um valor x5t, o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

c) O objeto CBOR/COSE resultante deve ser comprimido de acordo com o ponto 1, alínea d) do presente anexo. A carga útil do código QR deve consistir no prefixo «EP1:MDOC:», seguido da matriz de bytes comprimida resultante, e a carga útil completa deve ser codificada utilizando o formato binário como um único segmento de dados do código QR.

O conteúdo dos dados deve consistir num subconjunto de dados visíveis que figurem nos campos da parte da frente do cartão enumerados no anexo II da Diretiva (UE) 2024/2841 (data de expiração, número de série do cartão), juntamente com o identificador de revogação, a assinatura eletrónica e as informações sobre o esquema.

A assinatura eletrónica deve conter:

i) issuerAuth — objeto COSE_Sign1 assinado com a **chave privada QSealC** da autoridade emissora.

ii) cabeçalho protegido que inclui os valores alg = ES256 (algoritmo de assinatura) e x5t (o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

5. **Dados facultativos**

Não devem ser incluídos dados facultativos no código QR.

6. **Identificador de revogação**

O identificador de revogação do cartão europeu de estacionamento para pessoas com deficiência deve cumprir o disposto no anexo I, ponto 6.

As listas para cartões europeus de estacionamento para pessoas com deficiência revogados devem fazer referência apenas ao identificador de revogação. Os números de série dos cartões não podem ser publicados nas listas de revogação.

7. **Carga útil CBOR (dentro do QR) do cartão europeu de estacionamento para pessoas com deficiência**

Apenas os seguintes dados devem ser incluídos na carga útil do QR, em consonância com os campos visíveis do cartão europeu de estacionamento para pessoas com deficiência estabelecidos no anexo II da Diretiva (UE) 2024/2841:

Campo	caminho de acesso mDOC	Tipo/Formato
Versão do esquema de dados	issuerSigned.nameSpaces."eu.epc".ver	Cadeia de carateres alfanuméricos (p. ex., "1.0")
Tipo de cartão: cartão europeu de estacionamento para pessoas com deficiência	docType	Enum («eu.epc»)
Número de série do cartão	issuerSigned.nameSpaces."eu.epc".sub	Cadeia de carateres alfanuméricos
Identificador de revogação	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bytes)
Data de validade do cartão	issuerSigned.nameSpaces."eu.epc".exp	Etiqueta CBOR 1004, conforme definida no RFC 8943 (secção 2.1), que contém uma cadeia de carateres de texto com codificação UTF-8 que representa uma data completa RFC 3339 no formato AAAA-MM-DD

A assinatura eletrónica é transportada pelo issuerAuth (um objeto COSE_Sign1). A cadeia de certificados não pode ser incorporada na carga útil do código QR; em vez disso, o cabeçalho protegido COSE deve incluir um valor x5t, um código de identificação digital do certificado utilizado para localizar o QSealC correspondente na lista de certificados de confiança armazenada na memória cache do verificador.

8. **Exemplo de carga útil do código QR do cartão europeu de estacionamento para pessoas com deficiência: representação lógica comentada no estilo de notação de objetos JavaScript**

O exemplo que se segue é uma representação do esquema lógico do cartão europeu de deficiência em notação JSON que pode ser compreendida por humanos. Na prática, esta estrutura não pode ser compreendida por humanos, uma vez que:

a) É codificada no CBOR (RFC 8949, secção 3);

b) É assinada utilizando uma estrutura COSE_Sign1 sem etiqueta com uma carga útil separada (RFC 9052, secção 4);

c) Incluirá uma etiqueta CBOR 1004 com a data de expiração no formato de valor de data completa, de acordo com o RFC 8943 (secção 2.1);

d) Incluirá o parâmetro de cabeçalho protegido x5t, em conformidade com o RFC 9360, utilizando o SHA-256 sobre o QSealC de entidade final codificado em DER; e

e) É comprimida e pré-fixada com a cadeia de carateres EP1:MDOC: antes de ser codificada no código QR.

```
{
  // Apenas esquema lógico do cartão europeu de estacionamento para pessoas com deficiência, em formato JSON legível por humanos.
  // A carga útil real do código QR é CBOR determinístico e não JSON.
  "docType": "eu.epc", // credencial do cartão europeu de estacionamento para pessoas com deficiência. O valor docType está incluído, juntamente com
    // issuerSigned, na carga útil externa COSE_Sign1.

  "issuerSigned": {
    // Dados protegidos por issuerAuth; utilizado como carga útil separada.
    // Para a criação e verificação da assinatura, a carga útil externa separada abrange
```

```
  // docType e issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0", // perfil QR/versão do esquema

      // Número de série do cartão; definido pelo emitente, máx. 24 carateres.
      "sub": "EF123456789012345678 90GH",

      // Identificador de revogação: CBOR bstr real, 16 bytes/128 bits.
      // Apresentado aqui como 32 carateres hexadecimais para legibilidade.
      "rid": "4a8d9c11223344556677 8899aabbccdd",

      // A codificação CBOR real utiliza a etiqueta 1004 para a data completa RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Formulário efetivo: COSE_Sign1 sem etiqueta, não um objeto JSON.
  "type": "COSE_Sign1",
  "tagged": falso, // codificado sem etiqueta CBOR COSE_Sign1
  "payload": "detached", // O campo da carga útil COSE é CBOR nulo.

  "protectedHeader": {
    // alg: ES256; parâmetro de cabeçalho COSE equivalente 1 = -7.
    "alg": "ES256",

    // x5t: código de identificação digital do certificado; parâmetro de cabeçalho COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", valor de dispersão equivalente COSE -16

      // Valor de dispersão SHA-256 do QSealC de entidade final codificado em DER.
      // 32 bytes representados por 64 carateres hexadecimais.
      "hashValue":
      "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // em branco neste exemplo

  // Assinatura ES256 COSE: 64 bytes = 128 carateres hexadecimais.
  "signature":
  "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef"
}
}
```

9. **Utilização de mecanismos criptográficos**

A utilização de mecanismos criptográficos no contexto do presente anexo deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA).

ANEXO III

NOTIFICAÇÃO DAS INFORMAÇÕES A QUE SE REFERE O ARTIGO 6.º, n.º 2,

1. Os Estados-Membros devem fornecer à Comissão as seguintes informações sobre cada autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência:

   a) O nome da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   b) Um número de registo da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   c) Um endereço de correio eletrónico e número de telefone de contacto da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   d) Um ou mais certificados que possam ser utilizados para verificar o selo eletrónico criado pela autoridade ou pelo organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência que a autoridade ou organismo emite, e relativamente aos quais os dados de identificação certificados incluam o nome e o número de registo do emitente, conforme especificado nas alíneas a) e b), respetivamente;

   e) o URL da localização onde o emitente publica o estado de validade das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência.

2. Os Estados-Membros podem fornecer à Comissão as seguintes informações sobre cada autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência:

   a) O URL da página Web em que se apresentam as políticas e as condições da autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência aplicáveis à disponibilização e utilização das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência que a autoridade ou organismo disponibiliza;

   b) Se for caso disso, o URL da página Web em que se apresentam informações adicionais sobre a autoridade ou o organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência.

ANEXO IV

ESPECIFICAÇÕES TÉCNICAS PARA UMA LISTA DE REVOGAÇÃO DAS VERSÕES FÍSICAS DO CARTÃO EUROPEU DE DEFICIÊNCIA OU DO CARTÃO EUROPEU DE ESTACIONAMENTO PARA PESSOAS COM DEFICIÊNCIA

1. Para efeitos do presente anexo, o identificador deve corresponder ao identificador de revogação definido no anexo I, ponto 6, e no anexo II, ponto 6.

2. Deve ser implementada uma lista de revogação sob a forma de um *token* da lista de identificadores no formato CWT (RFC 8392, secção 7), em conformidade com a cláusula 5.2 da especificação relativa à lista de estado do *token* (draft--ietf-oauth-status-list-14), com as seguintes alterações:

   a) O valor do atributo-tipo deve ser "application/identifierlist+cwt";

   b) O atributo do prazo de validade deve estar respeitado;

   c) O atributo StatusList não deve estar presente no conjunto de atributos CWT;

   d) A estrutura IdentifierList definida no ponto 3 deve estar presente como um atributo no conjunto de atributos CWT estabelecidos que utilizem a chave 65530;

   e) O CWT deve ser um objeto COSE_Sign1 que utiliza, para o cálculo da assinatura, um algoritmo de assinatura em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA);

   f) O CWT deve conter o parâmetro da cadeia x5, conforme definido no RFC 9360 (secção 2), no cabeçalho protegido que contém o certificado ou a cadeia de certificados para verificar a assinatura da lista de revogação;

   g) O OID de utilização alargada da chave indicado na especificação da lista de estado do *token* (draft-ietf-oauth--status-list-14) pode ser utilizado para o certificado de assinatura da lista de identificadores e recomenda-se que os verificadores apoiem o OID de utilização alargada da chave indicado na especificação da lista de estado do *token* e que as infraestruturas da autoridade emissora não tornem crítico o campo de utilização alargada da chave quando utilizam o OID de utilização alargada da chave indicado na especificação da lista de estado do *token*.

3. A estrutura IdentifierList deve ser uma estrutura CBOR com a Concise Data Definition Language (CDDL) seguinte:

```
IdentifierList = {

  "identifiers": { * Identifier => IdentifierInfo },

  ? "aggregation_uri": Aggregation_uri,

  * Tstr = > RFU

}

IdentifierInfo = {

  (tstr/int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```