II

(Atos não legislativos)

DECISÕES

DECISÃO DE EXECUÇÃO (UE) 2020/1023 DA COMISSÃO

de 15 de julho de 2020

que altera a Decisão de Execução (UE) 2019/1765 no que diz respeito ao intercâmbio transfronteiras de dados entre as aplicações móveis nacionais de rastreio de contactos e de alerta no âmbito da luta contra a pandemia de COVID-19

(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 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços ([1]), nomeadamente o artigo 14.º, n.º 3,

Considerando o seguinte:

(1) O artigo 14.º da Diretiva 2011/24/UE prevê que a União apoie e promova a cooperação e o intercâmbio de informações entre os Estados-Membros no âmbito de uma rede voluntária composta pelas autoridades nacionais responsáveis pela saúde em linha («rede de saúde em linha») designadas pelos Estados-Membros.

(2) A Decisão de Execução (UE) 2019/1765 da Comissão ([2]) estabelece as normas para a criação, a gestão e o funcionamento da rede de autoridades nacionais responsáveis pela saúde em linha. No seu artigo 4.º, a decisão confia à rede de saúde em linha a tarefa de facilitar uma maior interoperabilidade dos sistemas nacionais de tecnologias da informação e da comunicação e a transferibilidade transfronteiras dos dados de saúde eletrónicos no âmbito dos cuidados de saúde transfronteiras.

(3) À luz da crise de saúde pública causada pela pandemia de COVID-19, vários Estados-Membros desenvolveram aplicações móveis que suportam o rastreio de contactos e permitem que os utilizadores dessas aplicações sejam alertados para que tomem as medidas adequadas, como a realização de testes ou o autoisolamento, caso tenham sido potencialmente expostos ao vírus através da proximidade de outro utilizador de tais aplicações, que tenha comunicado um diagnóstico positivo. Essas aplicações dependem da tecnologia Bluetooth para detetar a proximidade entre dispositivos. Como as restrições de viagem entre foram levantadas em junho de 2020, dever-se-á alcançar uma maior interoperabilidade dos sistemas nacionais de tecnologias da informação e comunicação entre os no âmbito da rede de saúde em linha através da implementação de uma infraestrutura digital que permita a interoperabilidade entre aplicações móveis nacionais de apoio ao rastreio de contactos e aos alertas.

([1]) JO L 88 de 4.4.2011, p. 45.

([2]) Decisão de Execução (UE) 2019/1765 da Comissão, de 22 de outubro de 2019, que estabelece as regras para a criação, a gestão e o funcionamento da rede de autoridades nacionais responsáveis pela saúde em linha e que revoga a Decisão de Execução 2011/890/EU (JO L 270 de 24.10.2019, p. 83).

(4) A Comissão tem apoiado os Estados-Membros no que respeita às aplicações móveis supramencionadas. Em 8 de abril de 2020, a Comissão adotou uma recomendação relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados (a «recomendação da Comissão») ([3]). Os Estados-Membros da rede de saúde em linha adotaram, com o apoio da Comissão, um conjunto de instrumentos comuns da UE para os Estados-Membros relativos a aplicações móveis de rastreio de contactos ([4]), assim como diretrizes de interoperabilidade aplicáveis às aplicações móveis aprovadas de rastreio de contactos na UE ([5]). O conjunto de instrumentos define as exigências nacionais que devem ser cumpridas pelas aplicações móveis nacionais de rastreio de contactos e de alerta, em particular que devem ser voluntárias, aprovadas pelas respetivas autoridades sanitárias nacionais, respeitadoras da privacidade e descontinuadas assim que já não forem necessárias. Dada a evolução mais recente da crise de COVID-19, a Comissão ([6]) e o Comité Europeu para a Proteção de Dados ([7]) emitiram cada um orientações sobre as aplicações móveis e as ferramentas de rastreio de contactos relativamente à proteção de dados. A conceção das aplicações móveis dos Estados-Membros e da infraestrutura digital que permite a sua interoperabilidade baseia-se no conjunto de instrumentos comuns da UE, nas orientações acima referidas e nas especificações técnicas acordadas na rede de saúde em linha.

(5) A fim de facilitar a interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta, foi desenvolvida uma infraestrutura digital com o apoio da Comissão pelos Estados-Membros que participam na rede de saúde em linha, que decidiram avançar com a sua cooperação neste domínio numa base voluntária, como ferramenta informática para o intercâmbio de dados. Esta infraestrutura digital é referida como o «portal federativo».

(6) A presente decisão estabelece disposições relativas ao papel dos Estados-Membros participantes e da Comissão no funcionamento do portal federativo para a interoperabilidade transfronteiras das aplicações móveis nacionais de rastreio de contactos e de alerta.

(7) O tratamento de dados pessoais de utilizadores de aplicações móveis de rastreio de contactos e de alerta, que é efetuado sob a responsabilidade dos Estados-Membros ou de outras organizações públicas ou organismos oficiais dos Estados-Membros, deve ser efetuado em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([8]) («Regulamento Geral sobre a Proteção de Dados») e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([9]). O tratamento de dados pessoais efetuado sob a responsabilidade da Comissão para efeitos de gestão e garantia da segurança do portal federativo deve cumprir o disposto no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([10]).

(8) O portal federativo deve ser constituído por uma infraestrutura de TI segura que ofereça uma interface comum, onde as autoridades nacionais ou os organismos oficiais designados possam trocar um conjunto mínimo de dados relativos a contactos com pessoas infetadas pelo SARS-CoV-2, a fim de informar outras sobre a sua potencial exposição a essa infeção e promover uma cooperação eficaz em matéria de cuidados de saúde entre os Estados-Membros ao facilitar o intercâmbio de informações pertinentes.

(9) A presente decisão deve, portanto, estabelecer modalidades para o intercâmbio transfronteiras de dados entre as autoridades nacionais ou os organismos oficiais designados através do portal federativo dentro da UE.

([3]) Recomendação (UE) 2020/518 da Comissão, de 8 de abril de 2020, relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados (JO L 114 de 14.4.2020, p. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Comunicação da Comissão — Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (JO C 124I de 17.4.2020, p. 1).

([7]) Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19 e Declaração de 16 de junho de 2020 sobre o impacto na proteção de dados da interoperabilidade das aplicações de rastreio dos contactos, ambas disponíveis em: https://edpb.europa.eu

([8]) 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).

([9]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

([10]) 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).

(10) Os Estados-Membros participantes, representados pelas autoridades nacionais ou organismos oficiais designados, determinam em conjunto a finalidade e os meios de tratamento de dados pessoais através do portal federativo e constituem, por conseguinte, responsáveis conjuntos pelo tratamento. O artigo 26.º do Regulamento Geral sobre a Proteção de Dados impõe uma obrigação aos responsáveis conjuntos por operações de tratamento de dados no sentido de determinar, 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. Cada um dos responsáveis pelo tratamento deve assegurar que dispõe de uma base jurídica a nível nacional para o tratamento no âmbito do portal federativo.

(11) A Comissão, enquanto prestador de soluções técnicas e organizativas para o portal federativo, procede ao tratamento dos dados pessoais sob pseudónimo em nome dos Estados-Membros participantes no portal federativo enquanto responsáveis conjuntos pelo tratamento e é, por conseguinte, um subcontratante. Nos termos do artigo 28.º do Regulamento Geral sobre a Proteção de Dados 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. A presente decisão define regras que regulam o tratamento por parte da Comissão enquanto subcontratante.

(12) Ao proceder ao tratamento dos dados pessoais no âmbito do portal federativo, a Comissão encontra-se vinculada pela Decisão (UE, Euratom) 2017/46 da Comissão ([11]).

(13) Tendo em conta que os fins para os quais os responsáveis pelo tratamento de dados pessoais tratam os dados no âmbito das aplicações móveis nacionais de rastreio de contactos e de alerta não exigem necessariamente a identificação de um titular dos dados, os responsáveis pelo tratamento poderão nem sempre estar em condições de assegurar a aplicação dos direitos desses titulares. Os direitos referidos nos artigos 15.º a 20.º do Regulamento Geral sobre a Proteção de Dados podem, por conseguinte, não se aplicar sempre que estejam preenchidas as condições previstas no artigo 11.º desse regulamento.

(14) O anexo em vigor da Decisão de Execução (EU) 2019/1765 deve ser renumerado devido ao aditamento de dois novos anexos.

(15) A Decisão de Execução (EU) 2019/1765 deve, por conseguinte, ser alterada em conformidade.

(16) Dada a urgência da situação relacionada com a pandemia de COVID-19, a presente decisão deve ser aplicável a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

(17) 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 9 de julho de 2020.

(18) As medidas previstas na presente decisão estão em conformidade com o parecer do comité instituído pelo artigo 16.º da Diretiva 2011/24/UE,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

A Decisão de Execução (EU) 2019/1765 é alterada do seguinte modo:

1) No artigo 2.º, ponto 1, são inseridas as seguintes alíneas g), h), i), j), k), l), m), n) e o):

«g) "Utilizador da aplicação", a pessoa na posse de um dispositivo inteligente que tenha descarregado e que aciona uma aplicação móvel aprovada de rastreio de contactos e de alerta;

h) "Rastreio de contactos", as medidas aplicadas a fim de localizar as pessoas que tenham sido expostas a uma fonte de uma ameaça transfronteiriça grave para a saúde na aceção do artigo 3.º, alínea c), da Decisão 1082/2013/UE do Parlamento Europeu e do Conselho (*);

([11]) Decisão (UE, Euratom) 2017/46 da Comissão, de 10 de janeiro de 2017, relativa à segurança dos sistemas de comunicação e de informação na Comissão Europeia (JO L 6 de 11.1.2017, p. 40). 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.

i) "Aplicação móvel nacional de rastreio de contactos e de alerta", uma aplicação informática aprovada a nível nacional que funciona em dispositivos inteligentes, nomeadamente telemóveis inteligentes, concebida geralmente para uma interação abrangente e específica com recursos Web, que trata dados de proximidade e outras informações contextuais recolhidas por vários sensores presentes nos dispositivos inteligentes para efeitos de rastreio de contactos com pessoas infetadas com SARS-CoV-2 e que alerta as pessoas que possam ter estado expostas ao SARS-CoV-2. Estas aplicações móveis são capazes de detetar a presença de outros dispositivos que utilizem Bluetooth e procedem ao intercâmbio de informações com servidores de suporte utilizando a Internet;

j) "Portal federativo", um portal de acesso à rede gerido pela Comissão através de uma ferramenta informática segura que recebe, armazena e disponibiliza um conjunto mínimo de dados pessoais entre os servidores de suporte dos Estados-Membros para efeitos de assegurar a interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta;

k) "Chave", um identificador único efémero relativo a um utilizador da aplicação que comunique ter sido infetado com SARS-CoV-2, ou que possa ter sido exposto ao SARS-CoV-2;

l) "Verificação da infeção", o método aplicado para confirmar uma infeção com SARS-CoV-2, nomeadamente se foi comunicada pelo próprio utilizador da aplicação ou resultou de confirmação por parte de uma autoridade sanitária nacional ou de um teste laboratorial;

m) "Países de interesse", o Estado-Membro ou os Estados-Membros onde o utilizador da aplicação esteve nos 14 dias anteriores à data de carregamento das chaves e onde descarregou a aplicação móvel nacional aprovada de rastreio de contactos e de alerta e/ou onde viajou;

n) "País de origem das chaves", o Estado-Membro onde está localizado o servidor de suporte que carregou as chaves para o portal federativo;

o) "Histórico", um registo automático de uma atividade relacionada com o intercâmbio e o acesso a dados tratados através do portal federativo, que revele, nomeadamente, o tipo de atividade de tratamento, a data e hora da atividade de tratamento e o identificador da pessoa que efetua o tratamento dos dados.

(*) Decisão n.º 1082/2013/UE, do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, relativa às ameaças sanitárias transfronteiriças graves e que revoga a Decisão n.º 2119/98/CE (JO L 293 de 5.11.2013, p. 1).»

2) No artigo 4.º, n.º 1, é inserida a seguinte alínea h):

«h) Dar orientações aos Estados-Membros sobre o intercâmbio transfronteiras de dados pessoais através do portal federativo entre as aplicações móveis nacionais de rastreio de contactos e de alerta.».

3) No artigo 6.º, n.º 1, são aditadas as seguintes alíneas f) e g):

«f) Desenvolver, aplicar e manter medidas técnicas e organizativas apropriadas relacionadas com a segurança da transmissão e do alojamento de dados pessoais no portal federativo para efeitos de assegurar a interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta;

g) Apoiar a rede de saúde em linha a chegar a acordo sobre a conformidade técnica e organizativa das autoridades nacionais com os requisitos para o intercâmbio transfronteiras de dados pessoais no portal federativo, fornecendo e efetuando os testes e auditorias necessários. Os peritos dos Estados-Membros podem dar assistência aos auditores da Comissão.».

4) O artigo 7.º é alterado do seguinte modo:

a) O título é substituído por «Proteção de dados pessoais tratados através da infraestrutura de serviços digitais de saúde em linha»;

b) No n.º 2, o termo «anexo» é substituído por «anexo I».

5) É inserido o seguinte artigo 7.º-A:

«*Artigo 7.º-A*

Intercâmbio transfronteiras de dados através do portal federativo entre as aplicações móveis nacionais de rastreio de contactos e de alerta

1. Sempre que há intercâmbio de dados pessoais através do portal federativo, o seu tratamento deve ser limitado aos fins de facilitação da interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta no âmbito desse portal e da continuidade do rastreio de contactos no contexto transfronteiras.

2. Os dados pessoais referidos no n.º 3 devem ser transmitidos ao portal federativo num formato sob pseudónimo.

3. Os dados pessoais sob pseudónimo que sejam trocados através do portal federativo e aí tratados devem incluir apenas as seguintes informações:

a) as chaves transmitidas pelas aplicações móveis nacionais de rastreio de contactos e de alerta até 14 dias antes da data de carregamento das chaves;

b) os históricos associados às chaves em consonância com o protocolo das especificações técnicas utilizado no país de origem das chaves;

c) a verificação da infeção;

d) os países de interesse e o país de origem das chaves.

4. As autoridades nacionais ou os organismos oficiais designados que tratem os dados pessoais no portal federativo devem ser responsáveis conjuntos pelos dados tratados no portal federativo. As responsabilidades respetivas dos responsáveis conjuntos pelo tratamento são atribuídas em conformidade com o anexo II. Cada Estado-Membro que pretenda participar no intercâmbio transfronteiras de dados entre as aplicações móveis nacionais de rastreio de contactos e de alerta deve notificar a Comissão, antes de aderir, da sua intenção, e indicar qual a autoridade nacional ou organismo oficial designado enquanto responsável conjunto pelo tratamento.

5. A Comissão é o subcontratante de dados pessoais tratados no portal federativo. Na sua qualidade de subcontratante, a Comissão assegura a segurança do tratamento, incluindo a transmissão e o alojamento de dados pessoais no portal federativo e cumpre as obrigações de um subcontratante estabelecidas no anexo III.

6. A eficácia das medidas técnicas e organizativas no sentido de assegurar a segurança do tratamento de dados pessoais no portal federativo deve ser regularmente testada, apreciada e avaliada pela Comissão e pelas autoridades nacionais autorizadas a aceder ao portal federativo.

7. Sem prejuízo da decisão dos responsáveis conjuntos pelo tratamento de porem termo ao tratamento no âmbito do portal federativo, o funcionamento desse portal deve ser desativado pelo menos 14 dias depois de todas as aplicações móveis nacionais de rastreio de contactos e de alerta conectadas cessarem de transmitir chaves através do portal federativo.»

6) O anexo passa a ser designado por «anexo I».

7) São aditados os anexos II e III, cujo texto consta do anexo à presente Decisão.

Artigo 2.º

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

Feito em Bruxelas, em 15 de julho de 2020.

Pela Comissão

A Presidente

Ursula VON DER LEYEN

ANEXO

À Decisão de Execução 2019/1765 são aditados os seguintes anexos II e III:

«*ANEXO II*

RESPONSABILIDADES DOS ESTADOS-MEMBROS PARTICIPANTES ENQUANTO RESPONSÁVEIS CONJUNTOS PELO TRATAMENTO DO PORTAL FEDERATIVO PARA O TRATAMENTO TRANSFRONTEIRAS ENTRE APLICAÇÕES MÓVEIS NACIONAIS DE RASTREIO DE CONTACTOS E DE ALERTA

SECÇÃO 1

Subsecção 1

Divisão de responsabilidades

1) Os responsáveis conjuntos procedem ao tratamento dos dados pessoais através do portal federativo em conformidade com as especificações técnicas estipuladas pela rede de saúde em linha ([1]).

2) Cada responsável pelo tratamento é responsável pelo tratamento de dados pessoais no portal federativo em conformidade com o Regulamento Geral sobre a Proteção de Dados e com a Diretiva 2002/58/CE.

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

4) Um subgrupo temporário criado pela rede de saúde em linha em conformidade com o artigo 5.º, n.º 4, será encarregado de analisar quaisquer questões decorrentes da interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta e da responsabilidade conjunta do tratamento correlato de dados pessoais e de facultar instruções coordenadas à Comissão enquanto subcontratante. Entre outras questões, os responsáveis pelo tratamento podem, no âmbito do subgrupo temporário, trabalhar no sentido de uma abordagem comum no que respeita à conservação de dados nos seus servidores de suporte nacionais, tendo em conta o período de conservação estabelecido no portal federativo.

5) As instruções ao subcontratante devem ser enviadas por qualquer ponto de contacto dos responsáveis conjuntos pelo tratamento, com o acordo dos outros responsáveis conjuntos pelo tratamento no âmbito do subgrupo anteriormente referido.

6) Somente as pessoas autorizadas pelas autoridades nacionais ou organismos oficiais designados podem aceder aos dados pessoais dos utilizadores intercambiados no portal federativo.

7) Cada autoridade nacional ou organismo oficial designado deixa de ser responsável conjunto pelo tratamento a partir da data de retirada da sua participação do portal federativo. Permanece, contudo, responsável pelo tratamento no portal federativo antes da sua retirada.

Subsecção 2

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

1) Cada responsável pelo tratamento deve fornecer aos utilizadores da sua aplicação móvel nacional de rastreio de contactos e de alerta («os titulares dos dados») informações sobre o tratamento dos seus dados pessoais no portal federativo para efeitos de interoperabilidade transfronteiras das aplicações móveis nacionais de rastreio de contactos e de alerta, em conformidade com os artigos 13.º e 14.° do Regulamento Geral sobre a Proteção de Dados.

2) Cada responsável pelo tratamento atua como ponto de contacto para os utilizadores da sua aplicação móvel nacional de rastreio de contactos e de alerta e tramita os pedidos relacionados com o exercício dos direitos dos titulares dos dados em conformidade com o Regulamento Geral sobre a Proteção de Dados, submetidos por esses utilizadores ou pelos seus representantes. Cada responsável pelo tratamento nomeia um ponto de contacto específico dedicado aos pedidos recebidos dos titulares dos dados. Caso um responsável conjunto pelo tratamento receba um pedido de um titular de dados que não seja da sua responsabilidade, deve de imediato remetê-lo para o responsável conjunto pelo tratamento adequado. Se tal for solicitado, os responsáveis conjuntos pelo tratamento de dados devem prestar-se assistência recíproca na tramitação dos pedidos dos titulares dos dados e devem responder uns aos outros sem atrasos indevidos e o mais tardar no prazo de 15 dias a contar da receção de um pedido de assistência.

([1]) Em particular, as especificações de interoperabilidade para as cadeias de transmissão transfronteiras entre as aplicações aprovadas, de 16 de junho de 2020, disponíveis em: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

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

SECÇÃO 2

Gestão de incidentes de segurança, incluindo violações de dados pessoais

1) Os responsáveis conjuntos pelo tratamento devem assistir-se reciprocamente na identificação e no tratamento de quaisquer incidentes de segurança, incluindo violações de dados pessoais, ligados ao tratamento no portal federativo.

2) Em particular, os responsáveis conjuntos pelo tratamento devem notificar-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 federativo;

b) quaisquer incidentes de segurança associados à operação de tratamento no portal federativo;

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

d) qualquer violação de salvaguardas técnicas e/ou organizativas das operações de tratamento no portal federativo.

3) Os responsáveis conjuntos pelo tratamento comunicam eventuais violações de dados 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 (UE) 2016/679 ou após notificação pela Comissão.

SECÇÃO 3

Avaliação de impacto sobre a proteção de dados

Caso um responsável pelo tratamento, de molde a cumprir as suas obrigações especificadas nos artigos 35.º e 36.º do Regulamento Geral sobre a Proteção de Dados, precisar de informações de outro responsável pelo tratamento, deve enviar um pedido específico para a caixa de correio funcional referida na secção 1, subsecção 1(3). Este último responsável pelo tratamento deve envidar os seus melhores esforços para prestar tais informações.

ANEXO III

RESPONSABILIDADES DA COMISSÃO ENQUANTO SUBCONTRATANTE DO TRATAMENTO DE DADOS DO PORTAL FEDERATIVO PARA O TRATAMENTO TRANSFRONTEIRAS ENTRE APLICAÇÕES MÓVEIS NACIONAIS DE RASTREIO DE CONTACTOS E DE ALERTA

A Comissão:

1) Estabelece e assegura a segurança e a fiabilidade de uma infraestrutura de comunicação que interliga as aplicações móveis nacionais de rastreio de contactos e de alerta dos Estados-Membros que participam no portal federativo. A fim de cumprir as suas obrigações enquanto subcontratante de dados do portal federativo, a Comissão pode contratar terceiros como subcontratantes; a Comissão 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, tal como definido no anexo II, secção 1, subsecção 1(4). A Comissão deve assegurar que esses subcontratantes cumpram as mesmas obrigações em matéria de proteção de dados estabelecidas na presente decisão.

2) 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 pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público.

3) O tratamento efetuado pela Comissão implica o seguinte:

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

b) receção dos dados referidos no artigo 7.º-A, n.º 3, da decisão de execução carregados pelos servidores de suporte nacionais pela prestação de uma interface de programação de aplicações que permita aos servidores de suporte nacionais carregar os dados pertinentes;

c) armazenamento dos dados no portal federativo, após sua receção a partir dos servidores de suporte nacionais;

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

e) supressão dos dados quando todos os servidores de suporte nacionais os tiverem descarregado ou 14 dias após a sua receção, consoante o que ocorrer primeiro.

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

O subcontratante deve tomar as medidas necessárias para preservar a integridade dos dados tratados.

4) Toma todas as medidas de segurança mais avançadas ao nível organizacional, físico e lógico para manter o portal federativo. Para esse efeito, a Comissão:

a) designa uma entidade responsável pela gestão da segurança ao nível do portal federativo, comunica aos responsáveis pelo tratamento os seus dados de contacto e assegura a sua disponibilidade para reagir a ameaças à segurança;

b) assume a responsabilidade pela segurança do portal federativo;

c) assegura que todas as pessoas a quem é concedido acesso ao portal federativo 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 implementa procedimentos específicos relacionados com a ligação dos servidores de suporte ao portal federativo. Tal inclui:

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

b) um procedimento de auditoria e revisão para:

   i) verificar a correspondência entre as medidas de segurança implementadas e a política de segurança aplicável;

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

   iii) acompanhar a deteção de ruturas de segurança e intrusões;

   iv) implementar alterações para evitar vulnerabilidades de segurança existentes

   v) permitir, incluindo a pedido dos responsáveis pelo tratamento, e contribuir 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 ([2]);

([2]) Protocolo (N.o 7) relativo aos privilégios e imunidades da União Europeia (JO C 326 de 26.10.2012, p. 266).

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

d) 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) Um procedimento para incidentes de segurança com vista a definir o sistema de notificação e escalonamento, informar sem demora os responsáveis pelo tratamento, bem como a Autoridade Europeia para a Proteção de Dados, de qualquer rutura da segurança e definir um processo disciplinar para lidar com ruturas da segurança.

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

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

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

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

d) assegura que os equipamentos não podem ser adicionados, substituídos ou retirados sem autorização prévia dos organismos competentes designados;

e) controla o acesso de e para os servidores de suporte ao portal federativo;

f) garante que as pessoas que têm acesso ao portal federativo são identificadas e autenticadas;

g) revê os direitos de autorização relacionados com o acesso ao portal federativo em caso de rutura da segurança que afete esta infraestrutura;

h) mantém a integridade das informações transmitidas através do portal federativo;

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 federativo a partir do domínio das autoridades nacionais (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 seu portal federativo, elabora estatísticas regulares e mantém registos.

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

11) Assiste os responsáveis pelo tratamento através de medidas técnicas e organizativas adequadas, na medida do possível, para o cumprimento da obrigação do responsável pelo tratamento de responder aos pedidos de exercício dos direitos do titular de dados estabelecidos no capítulo III do Regulamento Geral sobre a Proteção de Dados.

12) Apoia os responsáveis pelo tratamento ao prestar informações sobre o portal federativo, de forma a cumprir as obrigações decorrentes dos artigos 32.º, 35.º e 36.º do Regulamento Geral sobre a Proteção de Dados.

13) Assegura que os dados tratados no âmbito do portal federativo 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 federativo 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 federativo.

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