Diretrizes

# Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19

## Adotadas em 21 de abril de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

## Histórico das versões

| | | |
|---|---|---|
| Versão 1.1 | 5 de maio de 2020 | Correções menores |
| Versão 1.0 | 12 de abril de 2020 | Adoção das Diretrizes |

# Índice

## O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n.º 1, alínea e), do 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 (a seguir designado por «RGPD»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta os artigos 12.º e 22.º do seu Regulamento Interno,

**ADOTOU AS SEGUINTES DIRETRIZES:**

# 1 INTRODUÇÃO E CONTEXTO

1 Os governos e intervenientes privados estão a ponderar o recurso a soluções baseadas em dados como parte da resposta à pandemia de COVID-19, o que suscita inúmeras preocupações em matéria de privacidade.

2 O CEPD sublinha que o quadro jurídico da proteção de dados foi concebido para ser flexível e, como tal, é suscetível de dar uma resposta eficaz tanto no que se refere à limitação da pandemia como à proteção dos direitos humanos e das liberdades fundamentais.

3 O CEPD acredita firmemente que, quando o tratamento de dados pessoais é necessário para gerir a pandemia de COVID-19, a proteção de dados é indispensável para gerar confiança, criar as condições favoráveis à aceitação social de qualquer solução e garantir assim a eficácia destas medidas. Uma vez que o vírus não conhece fronteiras, parece preferível desenvolver uma abordagem europeia comum em resposta à atual crise ou, pelo menos, criar um quadro interoperável.

4 O CEPD considera, de um modo geral, que os dados e a tecnologia utilizados para ajudar a combater a COVID-19 devem ser utilizados para capacitar, e não para controlar, estigmatizar ou reprimir os cidadãos. Além disso, embora os dados e a tecnologia possam ser instrumentos importantes, têm limitações intrínsecas e podem apenas aumentar a eficácia de outras medidas de saúde pública. Os princípios gerais de eficácia, necessidade e proporcionalidade devem orientar qualquer medida adotada pelos Estados-Membros ou pelas instituições da UE que envolva o tratamento de dados pessoais para combater a COVID-19.

5 As presentes diretrizes esclarecem as condições e os princípios para a utilização proporcionada de dados de localização e meios de rastreio de contactos para dois fins específicos:

- a utilização de dados de localização para apoiar a resposta à pandemia, através da modelização da propagação do vírus de modo a avaliar a eficácia global das medidas de confinamento;
- o rastreio de contactos, que visa notificar os cidadãos do facto de terem estado na proximidade imediata de alguém que veio a confirmar-se ser portador do vírus, a fim de quebrar as cadeias de contaminação o mais rapidamente possível.

1 As referências a «Estados-Membros» ao longo do presente documento devem entender-se como referências a «Estados-Membros do EEE».

6 A eficácia da contribuição das aplicações de rastreio de contactos para a gestão da pandemia depende de muitos fatores (por exemplo, da percentagem de pessoas que teriam de instalá-las; da definição de «contacto» em termos de proximidade e duração). Além disso, é necessário que tais aplicações façam parte de uma estratégia abrangente em matéria de saúde pública para combater a pandemia, incluindo, nomeadamente, a realização de testes e o subsequente rastreio manual de contactos com o intuito de dissipar dúvidas. A sua implantação deve ser acompanhada de medidas de apoio para assegurar que as informações fornecidas aos utilizadores sejam contextualizadas e que os alertas possam ser úteis para o sistema público de saúde. Caso contrário, estas aplicações podem não produzir plenamente os seus efeitos.

7 O CEPD salienta que tanto o RGPD como a Diretiva 2002/58/CE (a seguir designada por «a diretiva») contêm regras específicas que permitem a utilização de dados anónimos ou pessoais para apoiar as autoridades públicas e outros intervenientes a nível nacional e da UE na monitorização e contenção da propagação do vírus SARS-CoV-2[2].

8 A este respeito, o CEPD já tomou posição sobre o facto de a utilização de aplicações de rastreio de contactos dever ser voluntária e não dever depender do rastreio de movimentos individuais, mas sim de informações sobre a proximidade dos utilizadores[3].

[2] Ver a declaração anterior proferida pelo CEPD sobre o surto de COVID-19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

# 2 UTILIZAÇÃO DE DADOS DE LOCALIZAÇÃO

## 2.1 Fontes de dados de localização

9 Há duas fontes principais de dados de localização disponíveis para modelizar a propagação do vírus e a eficácia global das medidas de confinamento:

- os dados de localização recolhidos por prestadores de serviços de comunicações eletrónicas (como operadores de telecomunicações móveis) no decurso da prestação do seu serviço; e
- os dados de localização recolhidos pelas aplicações dos prestadores de serviços da sociedade da informação cuja funcionalidade exige a utilização de tais dados (por exemplo, navegação, serviços de transporte, etc.).

10 O CEPD recorda que os dados de localização[4] recolhidos junto dos prestadores de serviços de comunicações eletrónicas só podem ser tratados no âmbito do disposto nos artigos 6.º e 9.º da diretiva. Tal significa que estes dados só podem ser transmitidos a autoridades ou outras partes terceiras se tiverem sido anonimizados pelo prestador ou, no caso dos dados que indiquem a posição geográfica do equipamento terminal de um utilizador, que não sejam dados de tráfego, com o consentimento prévio dos utilizadores[5].

11 No que se refere às informações, incluindo os dados de localização, recolhidas diretamente do equipamento terminal, é aplicável o disposto no artigo 5.º, n.º 3, da diretiva. Assim, o armazenamento de informações no dispositivo do utilizador ou a possibilidade de acesso a informações já armazenadas no mesmo só são permitidos se i) o utilizador tiver dado o seu consentimento[6] ou ii) o armazenamento e/ou o acesso forem estritamente necessários para prestar o serviço da sociedade da informação expressamente solicitado pelo utilizador.

12 No entanto, são permitidas derrogações dos direitos e das obrigações previstas na diretiva nos termos do artigo 15.º, sempre que as mesmas constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para alcançar determinados objetivos[7].

13 Quanto à reutilização dos dados de localização recolhidos por um prestador de serviços da sociedade da informação para fins de modelização (por exemplo, através do sistema operativo ou de alguma aplicação previamente instalada), devem ser satisfeitas condições adicionais. De facto, quando os dados tiverem sido recolhidos em conformidade com o disposto no artigo 5.º, n.º 3, da diretiva, os mesmos só poderão ser tratados posteriormente com o consentimento adicional do titular dos dados ou com base em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, do RGPD[8].

## 2.2 Enfoque na utilização de dados de localização anonimizados

14 O CEPD salienta que, quando se trata de utilizar dados de localização, deve ser sempre dada preferência ao tratamento de dados anonimizados em vez de dados pessoais.

15 A anonimização refere-se à utilização de um conjunto de técnicas a fim de impedir que se possa estabelecer uma ligação entre os dados e uma pessoa singular identificada ou identificável mediante um esforço «razoável». Este «teste de razoabilidade» deve ter em conta tanto aspetos

---

[4] Ver artigo 2.º, alínea c), da diretiva.
[5] Ver artigos 6.º e 9.º da diretiva.
[6] A noção de consentimento constante da diretiva continua a ser a mesma noção de consentimento constante do RGPD e deve cumprir todos os requisitos em matéria de consentimento, tal como previsto no artigo 4.º, n.º 11, e no artigo 7.º, do RGPD.
[7] Para a interpretação do artigo 15.º da diretiva, ver também o acórdão do Tribunal de Justiça da União Europeia (TJUE) de 29 de janeiro de 2008, Productores de Música de España (Promusicae)/Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54.
[8] Ver secção 1.5.3 das Orientações 1/2020 sobre o tratamento de dados pessoais no contexto de veículos conectados (*Guidelines 1/2020 on processing personal data in the context of connected vehicles*).

objetivos (tempo, meios técnicos) como elementos contextuais que podem variar caso a caso (raridade de um fenómeno, tendo em conta, por exemplo, densidade populacional, natureza e volume de dados). Se os dados não passarem neste teste significa que não foram anonimizados, pelo que continuarão a ser abrangidos pelo âmbito de aplicação do RGPD.

16 A avaliação da solidez da anonimização baseia-se em três critérios: i) seleção (isolar uma pessoa dentro de um grupo maior com base nos dados); ii) possibilidade de estabelecer uma ligação (ligar dois registos relativos à mesma pessoa); e iii) inferência (deduzir, com uma probabilidade significativa, informações desconhecidas sobre uma pessoa).

17 O conceito de anonimização é propenso a ser mal compreendido, sendo frequentemente confundido com pseudonimização. Enquanto a anonimização permite a utilização dos dados sem qualquer restrição, os dados pseudonimizados continuam a ser abrangidos pelo âmbito de aplicação do RGPD.

18 Existem muitas opções para uma anonimização eficaz[9], mas com uma ressalva. Os dados não podem ser anonimizados por si só, o que significa que apenas conjuntos de dados como um todo podem ou não ser tornados anónimos. Neste sentido, qualquer intervenção num único padrão de dados (por meio de cifragem ou quaisquer outras transformações matemáticas) pode, na melhor das hipóteses, ser considerada uma pseudonimização.

19 Os processos de anonimização e os ataques de reidentificação são domínios ativos de investigação. É crucial para qualquer responsável pelo tratamento de dados que implemente soluções de anonimização acompanhar as evoluções recentes neste domínio, especialmente no que diz respeito aos dados de localização (provenientes de operadores de telecomunicações e/ou serviços da sociedade da informação), que se sabe serem notoriamente difíceis de anonimizar.

20 Na verdade, uma grande quantidade de trabalhos de investigação mostrou[10] que *os dados de localização considerados anonimizados* podem, de facto, não o ser. Os sinais de mobilidade dos cidadãos estão intrínseca e altamente correlacionados e são únicos. Por conseguinte, podem ser vulneráveis a tentativas de reidentificação em determinadas circunstâncias.

21 Um único padrão de dados que rastreie a localização de um cidadão durante um período significativo não pode ser totalmente anonimizado. Esta apreciação ainda pode continuar a ser válida se a precisão das coordenadas geográficas registadas não for suficientemente reduzida, ou se pormenores do trajeto forem eliminados e mesmo que apenas seja mantida a localização dos locais em que o titular dos dados permanece durante um período considerável. Tal é igualmente válido para os dados de localização que sejam agregados de forma insuficiente.

22 Para alcançar a anonimização, os dados de localização devem ser cuidadosamente tratados a fim de passar no teste de razoabilidade. Neste sentido, tal tratamento inclui a tomada em consideração de conjuntos de dados de localização como um todo, bem como o tratamento de dados de um conjunto razoavelmente grande de indivíduos utilizando técnicas sólidas de anonimização que estejam disponíveis, desde que estas sejam aplicadas de forma adequada e eficaz.

23 Por último, dada a complexidade dos processos de anonimização, é altamente incentivada a transparência em relação à metodologia de anonimização.

---

[9] de Montjoye, Yves-Alexandre, e outros, «On the privacy-conscientious use of mobile phone data» [Sobre a utilização consciente em matéria de privacidade dos dados dos telefones móveis], 2018.
[10] de Montjoye, Yves-Alexandre, e outros, «Unique in the Crowd: The privacy bounds of human mobility» [Único na multidão: os limites da privacidade da mobilidade humana], 2013, e Pyrgelis, Apostolos, e outros, «Knock Knock, Who's There? Membership Inference on Aggregate Location Data» [Toc toc, Quem é? Inferência sobre dados de localização agregados], 2017.

# 3 APLICAÇÕES DE RASTREIO DE CONTACTOS

## 3.1 Análise jurídica geral

24 A monitorização sistemática e em grande escala da localização e/ou dos contactos entre pessoas singulares constitui uma grande invasão da sua privacidade que só pode ser legitimada se tiver por base uma adoção voluntária pelos utilizadores para cada uma das respetivas finalidades. Tal implicaria, em particular, que os cidadãos que decidissem não utilizar tais aplicações, ou que o não pudessem fazer, não fossem prejudicados de modo nenhum.

25 Para garantir a responsabilização, o responsável pelo tratamento de dados de qualquer aplicação de rastreio de contactos deve ser claramente definido. O CEPD considera que as autoridades nacionais de saúde poderiam ser os responsáveis pelo tratamento de dados[11] de uma tal aplicação, podendo igualmente ser previstos outros responsáveis pelo tratamento de dados. Em todo o caso, se a implantação de aplicações de rastreio de contactos envolver diferentes intervenientes, as suas funções e responsabilidades devem ser claramente definidas desde o início e explicadas aos utilizadores.

26 Além disso, no que diz respeito ao princípio da limitação da finalidade, os fins devem ser suficientemente específicos para excluir o tratamento posterior para finalidades não relacionadas com a gestão da crise sanitária da COVID-19 (por exemplo, fins comerciais ou de aplicação da lei). Uma vez definido claramente o objetivo, será necessário assegurar que a utilização dos dados pessoais seja adequada, necessária e proporcionada.

27 No contexto de uma aplicação de rastreio de contactos, devem ser devidamente tidos em consideração os princípios da minimização de dados e da proteção de dados desde a conceção e por defeito:

- as aplicações de rastreio de contactos não exigem o rastreio da localização de utilizadores individuais. Em vez disso, devem ser utilizados dados de proximidade;
- uma vez que as aplicações de rastreio de contactos podem funcionar sem a identificação direta de indivíduos, devem ser adotadas medidas adequadas para evitar a reidentificação;
- as informações recolhidas devem estar armazenadas no equipamento terminal do utilizador, devendo apenas ser recolhidas as informações pertinentes quando tal for absolutamente necessário.

28 No que se refere à licitude do tratamento, o CEPD observa que as aplicações de rastreio de contactos envolvem o armazenamento e/ou o acesso a informações já armazenadas no terminal, as quais estão sujeitas ao disposto no artigo 5.º, n.º 3, da diretiva. Se essas operações fossem estritamente necessárias para a prestação, pelo fornecedor da aplicação, do serviço explicitamente solicitado pelo utilizador, o tratamento não exigiria o seu consentimento. No que se refere a operações que não fossem estritamente necessárias, o fornecedor teria de obter o consentimento do utilizador.

29 Além disso, o CEPD observa que o simples facto de a utilização de aplicações de rastreio de contactos ter lugar numa base voluntária não significa que o tratamento de dados pessoais se baseie necessariamente no consentimento. Quando as autoridades públicas prestam um serviço com base num mandato conferido por e em consonância com os requisitos previstos na lei, afigura-se que a base jurídica mais pertinente para o tratamento é a necessidade de exercer funções de interesse público, nos termos do disposto no artigo 6.º, n.º 1, alínea e), do RGPD.

30 O artigo 6.º, n.º 3, do RGPD esclarece que o fundamento jurídico para o tratamento referido no artigo 6.º, n.º 1, alínea e), é definido pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse

[11] Ver também a Comunicação da Comissão Europeia — Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados, C(2020) 2523 final, 16.4.2020, Bruxelas.

fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento[12].

31 No entanto, a base jurídica ou medida legislativa que fornece o fundamento legal para a utilização de aplicações de rastreio de contactos deve incorporar salvaguardas significativas, incluindo uma referência ao caráter voluntário da aplicação. Deve ser incluída uma especificação clara da finalidade e limitações explícitas relativas à utilização posterior dos dados pessoais, bem como uma identificação clara do(s) responsável(eis) pelo tratamento de dados envolvido(s). Devem igualmente ser identificadas as categorias de dados, bem como as entidades a quem os dados pessoais podem ser divulgados (e as finalidades para as quais os dados pessoais podem ser divulgados). Dependendo do nível de interferência, devem ser incorporadas salvaguardas adicionais, tendo em conta a natureza, o âmbito e as finalidades do tratamento. Por último, o CEPD recomenda ainda a inclusão, logo que possível, dos critérios para determinar quando a aplicação deve ser desinstalada e que entidade deve ser responsável e responsabilizável por essa determinação.

32 No entanto, se o tratamento de dados assentar noutra base jurídica, como, por exemplo, o consentimento (artigo 6.º, n.º 1, alínea a)),[13] o responsável pelo tratamento de dados terá de assegurar o cumprimento dos requisitos rigorosos para que essa base jurídica seja válida.

33 Além disso, a utilização de uma aplicação para combater a pandemia de COVID-19 pode conduzir à recolha de dados relativos à saúde (por exemplo, sobre o estado de saúde de uma pessoa infetada). O tratamento de tais dados é permitido quando for necessário por motivos de interesse público no domínio da saúde pública, em cumprimento das condições previstas no artigo 9.º, n.º 2, alínea i), do RGPD[14], ou para efeitos de prestação de cuidados de saúde, conforme descrito no artigo 9.º, n.º 2, alínea h), do RGPD[15]. Dependendo da base jurídica, pode igualmente assentar no consentimento explícito (artigo 9.º, n.º 2, alínea a), do RGPD).

34 De acordo com a finalidade inicial, o artigo 9.º, n.º 2, alínea j), do RGPD permite ainda o tratamento de dados relativos à saúde quando este for necessário para fins de investigação científica ou para fins estatísticos.

35 A atual crise sanitária não deve ser utilizada como uma oportunidade para conferir mandatos desproporcionados para efeitos de conservação de dados. A limitação da conservação deve ter em consideração as verdadeiras necessidades e a pertinência médica (que pode incluir considerações epidemiológicas como o período de incubação, etc.), devendo os dados pessoais ser mantidos apenas durante a crise da COVID-19. Posteriormente, como regra geral, todos os dados pessoais devem ser apagados ou anonimizados.

36 O CEPD considera que tais aplicações não podem substituir, mas apenas apoiar, o rastreio manual de contactos realizado por profissionais de saúde pública qualificados, que podem determinar se os contactos próximos são suscetíveis de resultar ou não na transmissão do vírus (por exemplo, ao interagir com alguém protegido por equipamentos adequados – operadores de caixa, etc.) – ou não). O CEPD sublinha que os procedimentos e processos, incluindo os respetivos algoritmos executados pelas aplicações de rastreio de contactos, devem funcionar sob a supervisão rigorosa de pessoal qualificado, a fim de limitar a ocorrência de falsos positivos e falsos negativos. Em particular, a tarefa de prestar aconselhamento sobre os próximos passos não deve basear-se exclusivamente no tratamento automatizado.

---

[12] Ver considerando 41.

[13] Os responsáveis pelo tratamento de dados (especialmente as autoridades públicas) devem prestar especial atenção ao facto de o consentimento não dever ser considerado como tendo sido dado de livre vontade se o indivíduo não dispuser de uma escolha verdadeira que lhe permita recusar ou retirar o seu consentimento sem ser prejudicado.

[14] O tratamento deve basear-se no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

[15] Ver artigo 9.º, n.º 2, alínea h), do RGPD.

37 A fim de assegurar a sua equidade, responsabilidade e, de um modo mais geral, a sua conformidade com a legislação, os algoritmos devem ser passíveis de auditoria e devem ser regularmente revistos por peritos independentes. O código-fonte da aplicação deve ser tornado público para poder ser objeto de um escrutínio tão amplo quanto possível.

38 Até certo ponto, ocorrerão sempre falsos positivos. Uma vez que a identificação de um risco de infeção pode, provavelmente, ter um grande impacto nos cidadãos, obrigando-os, por exemplo, a permanecer em autoisolamento até terem sido testados e o resultado ter sido negativo, a capacidade de corrigir dados e/ou resultados de análises subsequentes é uma necessidade. É evidente que tal só deverá aplicar-se a cenários e implementações em que os dados sejam tratados e/ou armazenados de forma a que tal correção seja tecnicamente viável e que os efeitos adversos acima mencionados sejam suscetíveis de ocorrer.

39 Por último, o CEPD considera que deve ser realizada uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) antes da implementação de tal instrumento, uma vez que o tratamento é considerado suscetível de resultar num elevado risco (dados relativos à saúde, adoção antecipada em grande escala, monitorização sistemática, utilização de novas soluções tecnológicas)[16]. O CEPD recomenda vivamente a publicação de AIPD.

### 3.2 Recomendações e requisitos funcionais

40 De acordo com o princípio da minimização de dados, entre outras medidas de proteção de dados desde a conceção e por defeito[17], os dados objeto de tratamento devem ser limitados ao mínimo estritamente necessário. A aplicação não deve recolher informações não relacionadas ou não necessárias, que podem incluir o estado civil, identificadores de comunicações, elementos de diretórios de equipamentos, mensagens, registos de chamadas, dados de localização, identificadores de dispositivos, etc.

41 Os dados transmitidos por aplicações devem incluir apenas alguns identificadores únicos e pseudonimizados, gerados pela aplicação e específicos da mesma. Esses identificadores devem ser renovados regularmente, com uma frequência compatível com a finalidade de conter a propagação do vírus, devendo o seu número ser suficiente para limitar o risco de identificação e de rastreio físico dos cidadãos.

42 As implementações para efeitos de rastreio de contactos podem seguir uma abordagem centralizada ou descentralizada[18]. Ambas devem ser consideradas opções viáveis, desde que sejam aplicadas medidas de segurança adequadas, cada uma delas acompanhada de um conjunto de vantagens e desvantagens. Assim, a fase conceptual do desenvolvimento de aplicações deve incluir sempre uma análise minuciosa de ambos os conceitos, ponderando cuidadosamente os respetivos efeitos sobre a proteção/privacidade dos dados e os possíveis impactos sobre os direitos dos cidadãos.

43 Qualquer servidor envolvido no sistema de rastreio de contactos deve apenas recolher o histórico de contactos ou os identificadores pseudonimizados de utilizadores diagnosticados como infetados em consequência de uma avaliação adequada efetuada pelas autoridades de saúde e de uma ação voluntária do utilizador. Alternativamente, o servidor deve manter uma lista de identificadores pseudonimizados de utilizadores infetados ou o seu histórico de contactos apenas durante o tempo necessário para informar utilizadores potencialmente

---

[16] Ver o documento do Grupo de Trabalho do Artigo 29.º intitulado «Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 ».

[17] Ver o documento do CEPD intitulado «EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default» [Orientações 4/2019 sobre a proteção de dados desde a conceção e por defeito prevista no artigo 25.º do RGPD].

[18] Em geral, a solução descentralizada é mais consentânea com o princípio da minimização.

infetados sobre a sua exposição, e não deve tentar identificar utilizadores potencialmente infetados.

44 A adoção de uma metodologia global de rastreio de contactos que inclua tanto aplicações como o rastreio manual pode exigir, em alguns casos, o tratamento de informações adicionais. Neste contexto, estas informações adicionais devem permanecer no terminal do utilizador e só devem ser objeto de tratamento quando tal seja estritamente necessário e com o consentimento prévio e específico do seu titular.

45 Devem ser utilizadas técnicas criptográficas de última geração para proteger os dados armazenados em servidores e aplicações, bem como os intercâmbios entre aplicações e o servidor remoto. Deve igualmente recorrer-se à autenticação mútua entre a aplicação e o servidor.

46 A comunicação de utilizadores como estando infetados com SARS-CoV-2 na aplicação deve estar sujeita a uma autorização adequada, por exemplo, através de um código de utilização única vinculado a uma identidade pseudonimizada da pessoa infetada e associado a um laboratório de testes ou a um profissional de saúde. Se a confirmação não puder ser obtida de forma segura, não deve ser realizado nenhum tratamento de dados que pressuponha a validade do estado de saúde do utilizador.

47 O responsável pelo tratamento de dados, em colaboração com as autoridades públicas, tem de informar, de forma clara e explícita, os cidadãos sobre a ligação a utilizar para descarregar a aplicação oficial nacional de rastreio de contactos, a fim de atenuar o risco de os cidadãos utilizarem uma aplicação de terceiros.

# 4 CONCLUSÃO

48 O mundo enfrenta atualmente uma importante crise de saúde pública que exige respostas fortes, cujo impacto far-se-á sentir para além do atual estado de emergência que o mundo vive. O tratamento automatizado de dados e as tecnologias digitais podem ser componentes fundamentais na luta contra a COVID-19. No entanto, é preciso ter cuidado com o «efeito irreversível». Temos a responsabilidade de garantir que as medidas tomadas nestas circunstâncias extraordinárias sejam necessárias, limitadas no tempo, limitadas ao mínimo necessário e sujeitas a uma revisão periódica e genuína, bem como a uma avaliação científica.

49 O CEPD sublinha que não se deve ter de escolher entre uma resposta eficaz à atual crise e a proteção dos nossos direitos fundamentais: podemos alcançar ambos e, além disso, os princípios de proteção de dados podem desempenhar um papel muito importante na luta contra o vírus. A legislação europeia em matéria de proteção de dados permite a utilização responsável de dados pessoais para fins de gestão da saúde, garantindo simultaneamente que os direitos e as liberdades individuais não sofram qualquer deterioração no processo.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

# ANEXO – APLICAÇÕES DE RASTREIO DE CONTACTOS GUIA DE ANÁLISE

## 0. Declaração de exoneração de responsabilidade

As diretrizes a seguir apresentadas não são prescritivas nem exaustivas, e o único objetivo do presente guia consiste em fornecer orientações gerais aos responsáveis pela conceção e implementação de aplicações de rastreio de contactos. Outras soluções para além das aqui descritas podem ser utilizadas e lícitas, desde que respeitem o quadro jurídico pertinente (isto é, o RGPD e a diretiva).

Note-se igualmente que o presente guia é de caráter geral. Consequentemente, as recomendações e obrigações nele contidas não devem ser consideradas exaustivas. Qualquer avaliação deve ser efetuada caso a caso, podendo aplicações específicas exigir medidas adicionais não incluídas no presente guia.

## 1. Síntese

Em muitos Estados-Membros, as partes interessadas estão a ponderar a utilização de aplicações de*rastreio de contactos* para ajudar a população a descobrir se esteve em contacto com uma pessoa infetada com SARS-CoV-2.

As condições em que tais aplicações contribuiriam efetivamente para a gestão da pandemia ainda não foram estabelecidas. E seria necessário estabelecer estas condições antes de qualquer implementação das aplicações em causa. No entanto, é pertinente fornecer orientações que apresentem informações pertinentes às equipas de desenvolvimento a montante, para que a proteção de dados pessoais possa ser garantida desde a fase inicial de conceção.

Note-se que o presente guia é de caráter geral. Consequentemente, as recomendações e obrigações nele contidas não devem ser consideradas exaustivas. Qualquer avaliação deve ser efetuada caso a caso, podendo aplicações específicas exigir medidas adicionais não incluídas no presente guia. O objetivo do presente guia consiste em fornecer orientações gerais aos responsáveis pela conceção e implementação de aplicações de rastreio de contactos.

Alguns critérios podem ir além dos requisitos rigorosos decorrentes do quadro de proteção de dados. Estes visam garantir o mais elevado nível de transparência, a fim de favorecer a aceitação social de tais aplicações de rastreio de contactos.

Para o efeito, os responsáveis pela disponibilização de aplicações de rastreio de contactos devem ter em conta os seguintes critérios:

- A utilização de tal aplicação deve ser estritamente voluntária, não podendo condicionar o acesso a quaisquer direitos garantidos por lei. Os cidadãos devem ter pleno controlo, em todos os momentos, sobre os seus dados, e devem poder escolher livremente utilizar tal aplicação.
- As aplicações de rastreio de contactos são suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares e de exigir a realização de uma avaliação de impacto sobre a proteção de dados antes da sua implantação.

- Podem ser obtidas informações sobre a proximidade entre os utilizadores da aplicação sem os localizar. Este tipo de aplicação não necessita e, por conseguinte, não deve envolver a utilização de dados de localização.
- Quando um utilizador é diagnosticado como estando infetado com o vírus SARS-CoV-2, apenas as pessoas com quem o utilizador tenha estado em contacto próximo no período de conservação epidemiologicamente pertinente para o rastreio de contactos devem ser informadas.
- O funcionamento deste tipo de aplicação pode exigir, dependendo da arquitetura escolhida, a utilização de um servidor centralizado. Nesse caso, e em conformidade com os princípios da minimização de dados e da proteção de dados desde a conceção, os dados tratados pelo servidor centralizado devem ser limitados ao mínimo estritamente necessário:
    - Quando um utilizador é diagnosticado como estando infetado, as informações sobre os seus contactos próximos anteriores ou os identificadores transmitidos pela aplicação do utilizador só podem ser recolhidas com o seu consentimento. É necessário definir um método de verificação que permita afirmar que a pessoa está, de facto, infetada sem a identificar. Tecnicamente, tal pode ser conseguido alertando apenas os contactos após a intervenção de um profissional de saúde, por exemplo, utilizando um código especial de utilização única.
    - As informações armazenadas no servidor central não devem permitir que o responsável pelo tratamento de dados identifique utilizadores diagnosticados como estando infetados ou que com estes tenham estado em contacto, nem devem permitir inferir padrões de contacto não necessários para a determinação dos contactos pertinentes.
- O funcionamento deste tipo de aplicação exige a transmissão de dados que são lidos por dispositivos de outros utilizadores e a escuta destas transmissões:
    - É suficiente para trocar identificadores pseudonimizados entre os equipamentos móveis dos utilizadores (computadores, tábletes, relógios conectados, etc.), por exemplo, através da sua transmissão (nomeadamente através da tecnologia Bluetooth de baixo consumo de energia).
    - Os identificadores devem ser gerados através de processos criptográficos de última geração.
    - Os identificadores devem ser renovados regularmente para reduzir o risco de rastreio físico e de ataques de ligação.
- Este tipo de aplicação deve ser protegido para garantir processos técnicos seguros. Em especial:
    - A aplicação não deve transmitir aos utilizadores informações que lhes permitam inferir a identidade ou o diagnóstico de outros utilizadores. O servidor central não deve identificar os utilizadores, nem sobre eles inferir informações.

**Declaração de exoneração de responsabilidade**: os princípios supracitados estão relacionados com o alegado objetivo das aplicações de *rastreio de contactos*, e exclusivamente com este objetivo. Tais aplicações visam apenas informar automaticamente os cidadãos potencialmente expostos ao vírus (sem ter de os identificar). Os responsáveis pela aplicação e pela sua infraestrutura podem ser

controlados pela autoridade de supervisão competente. O seguimento da totalidade ou de parte das presentes diretrizes não é necessariamente suficiente para garantir o pleno respeito do quadro de proteção de dados.

## 2. Definições

| | |
|---|---|
| **Contacto** | Para uma aplicação de rastreio de contactos, um contacto é um utilizador que tenha tido uma interação com um utilizador confirmado como sendo portador do vírus e cuja duração e distância permitem inferir um risco de exposição significativa à infeção pelo vírus. Os parâmetros relativos à duração da exposição e à distância entre pessoas devem ser estimados pelas autoridades de saúde e podem ser definidos na aplicação. |
| **Dados de localização** | Todos os dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível (conforme definido na diretiva), bem como dados de outras fontes potenciais, relativos:<br>– à latitude, longitude ou altitude do equipamento terminal;<br>– à direção da viagem do utilizador; ou<br>– ao momento em que as informações de localização foram registadas. |
| **Interação** | No contexto da aplicação de rastreio de contactos, uma interação é definida como o intercâmbio de informações entre dois dispositivos localizados na proximidade imediata um do outro (no espaço e no tempo), dentro do alcance da tecnologia de comunicação utilizada (por exemplo, Bluetooth). Esta definição exclui a localização dos dois utilizadores envolvidos na interação. |
| **Portador do vírus** | No presente documento, consideram-se portadores do vírus os utilizadores que tenham sido testados e o resultado tenha sido positivo para o vírus e que tenham recebido um diagnóstico oficial de médicos ou de centros de saúde. |
| **Rastreio de contactos** | As pessoas que tenham estado em contacto próximo (de acordo com critérios a definir pelos epidemiologistas) com uma pessoa infetada com o vírus correm um risco significativo de também ser infetadas e, por sua vez, de infetar outras pessoas.<br>O rastreio de contactos é uma metodologia de controlo de doenças que enumera todas as pessoas que tenham estado na proximidade imediata de um portador do vírus, a fim de verificar se as pessoas em causa estão em risco de contrair a infeção e tomar as medidas sanitárias adequadas relativamente às mesmas. |

## 3. Considerações de caráter geral

| | |
|---|---|
| GEN-1 | A aplicação deve ser um instrumento complementar às técnicas tradicionais de rastreio de contactos (nomeadamente a realização de entrevistas a pessoas infetadas), isto é, deve fazer parte de um programa de saúde pública mais amplo. Deve ser utilizada apenas até que as técnicas de rastreio de contactos manuais pontuais possam gerir sozinhas a quantidade de novas infeções. |
| GEN-2 | O mais tardar quando as autoridades públicas competentes decidirem o «regresso à normalidade», deve ser instituído um procedimento para pôr termo à recolha de identificadores (desativação global da aplicação, instruções para desinstalação da aplicação, desinstalação automática, etc.) e ativar a eliminação de todos os dados recolhidos de todas as bases de dados (aplicações móveis e servidores). |
| GEN-3 | O código-fonte da aplicação e do seu servidor deve ser aberto e as especificações técnicas devem ser tornadas públicas, para que qualquer parte interessada possa auditar o código e, quando pertinente, contribuir para melhorar o código, corrigir eventuais erros e garantir a transparência no tratamento de dados pessoais. |
| GEN-4 | As fases de implantação da aplicação devem permitir validar progressivamente a sua eficácia do ponto de vista da saúde pública. Para o efeito, deve ser definido um protocolo de avaliação que especifique indicadores que permitam medir a eficácia da aplicação. |

**4. Finalidades**

| | |
|---|---|
| PUR-1 | A aplicação deve prosseguir a única finalidade de rastrear contactos para que as pessoas potencialmente expostas ao vírus SARS-CoV-2 possam ser alertadas e receber os cuidados necessários. Não deve ser utilizada para outra finalidade. |
| PUR-2 | A aplicação não deve ser desviada da sua utilização principal para efeitos de controlo do cumprimento das medidas de quarentena ou de confinamento e/ou do distanciamento social. |
| PUR-3 | A aplicação não deve ser utilizada para tirar conclusões sobre a localização dos utilizadores com base na sua interação e/ou em quaisquer outros meios. |

**5. Considerações de caráter funcional**

| | |
|---|---|
| FUNC-1 | A aplicação deve dispor de uma funcionalidade que permita aos utilizadores serem informados de que foram potencialmente expostos ao vírus, baseando-se esta informação na proximidade de um utilizador infetado dentro de uma janela temporal de X dias antes do teste de rastreio positivo (sendo o valor X definido pelas autoridades de saúde). |
| FUNC-2 | A aplicação deve fornecer recomendações aos utilizadores identificados como tendo estado potencialmente expostos ao vírus. Deve transmitir instruções |

| | |
|---|---|
| | sobre as medidas que devem seguir, e deve permitir que o utilizador solicite conselhos. Nesses casos, seria obrigatória uma intervenção humana. |
| FUNC-3 | O algoritmo que mede o risco de infeção tendo em conta fatores de distância e tempo, determinando assim quando um contacto tem de ser registado na lista de rastreio de contactos, deve ser ajustado de forma segura para ter em conta os conhecimentos mais recentes sobre a propagação do vírus. |
| FUNC-4 | **Os utilizadores devem ser informados caso tenham estado expostos ao vírus**, ou devem obter regularmente informações sobre se foram ou não expostos ao vírus, durante o período de incubação do vírus. |
| FUNC-5 | A aplicação deve ser interoperável com outras aplicações desenvolvidas nos Estados-Membros, de modo a que os utilizadores que viajam por diferentes Estados-Membros possam ser notificados de forma eficiente. |

## 6. Dados

| | |
|---|---|
| DATA-1 | Para que o rastreio de contactos possa ser realizado, a aplicação deve ser capaz de transmitir e receber dados através de tecnologias de comunicação de proximidade, como o Bluetooth de baixo consumo de energia. |
| DATA-2 | Os dados transmitidos devem incluir identificadores pseudo-aleatórios criptograficamente fortes, gerados pela aplicação e específicos da mesma. |
| DATA-3 | O risco de colisão entre identificadores pseudo-aleatórios deve ser suficientemente baixo. |
| DATA-4 | Os identificadores pseudo-aleatórios devem ser renovados regularmente, com uma frequência suficiente para limitar o risco de reidentificação, rastreio físico ou ligação de cidadãos, por qualquer pessoa, incluindo operadores de servidores centrais, outros utilizadores da aplicação ou terceiros mal-intencionados. Estes identificadores devem ser gerados pela aplicação do utilizador, possivelmente com base numa «semente» fornecida pelo servidor central. |
| DATA-5 | De acordo com o princípio da minimização de dados, a aplicação não deve recolher outros dados para além dos estritamente necessários para efeitos de rastreio de contactos. |
| DATA-6 | A aplicação não deve recolher dados de localização para fins de rastreio de contactos. Os dados de localização podem ser objeto de tratamento com o único propósito de permitir que a aplicação interaja com aplicações semelhantes noutros países, devendo a sua precisão ser limitada ao estritamente necessário para este propósito exclusivo. |
| DATA-7 | A aplicação não deve recolher dados relativos à saúde para além dos estritamente necessários para as finalidades da aplicação, exceto numa base facultativa e com o único objetivo de auxiliar no processo de tomada da decisão de informar o utilizador. |

| | |
|---|---|
| DATA-8 | Os utilizadores devem ser informados de todos os dados pessoais que serão recolhidos. Estes dados só devem ser recolhidos com a sua autorização. |

## 7. Propriedades técnicas

| | |
|---|---|
| TECH-1 | A aplicação deve recorrer a tecnologias disponíveis como a tecnologia de comunicação de proximidade (por exemplo, Bluetooth de baixo consumo de energia - *Bluetooth Low Energy*) para detetar utilizadores nas imediações do dispositivo que executa a aplicação. |
| TECH-2 | A aplicação deve manter o histórico de contactos de um utilizador no respetivo equipamento, durante um período limitado predefinido. |
| TECH-3 | A aplicação pode depender de um servidor central para implementar algumas das suas funcionalidades. |
| TECH-4 | A aplicação deve ter por base uma arquitetura que recorra, tanto quanto possível, aos dispositivos dos utilizadores. |
| TECH-5 | Por iniciativa dos utilizadores notificados como estando infetados com o vírus e após confirmação do seu estado de saúde por um profissional de saúde devidamente certificado, o seu histórico de contactos ou os seus próprios identificadores devem ser transmitidos ao servidor central. |

## 8. Segurança

| | |
|---|---|
| SEC-1 | A aplicação deve dispor de um mecanismo que permita verificar o estado de saúde dos utilizadores que indicam ter sido testados e o resultado ter sido positivo para o vírus SARS-CoV-2, por exemplo, fornecendo um código de utilização única associado a um laboratório de testes ou a um profissional de saúde. Se a confirmação não puder ser obtida de forma segura, os dados não devem ser objeto de tratamento. |
| SEC-2 | Os dados enviados para o servidor central devem ser transmitidos através de um canal seguro.<br>A utilização de serviços de notificação prestados por fornecedores de plataformas OS deve ser cuidadosamente avaliada e não deve conduzir à divulgação de quaisquer dados a terceiros. |
| SEC-3 | As solicitações não devem ser vulneráveis à adulteração por um utilizador mal-intencionado. |
| SEC-4 | Devem ser implementadas técnicas criptográficas de última geração para assegurar intercâmbios entre a aplicação e o servidor e entre aplicações e, como regra geral, para proteger as informações armazenadas nas aplicações e no servidor. Entre os exemplos de técnicas que podem ser utilizadas incluem-se, por exemplo: a cifragem simétrica e assimétrica, funções de dispersão, o teste de pertença a uma associação privada, a intersecção de conjuntos privados, filtros de Bloom, recuperação de informações privadas, cifragem homomórfica, etc. |

| | |
|---|---|
| SEC-5 | O servidor central não deve manter identificadores de conexão de rede (por exemplo, endereços IP) de quaisquer utilizadores, incluindo dos que foram diagnosticados como estando infetados e que transmitiram o seu histórico de contactos ou os seus próprios identificadores. |
| SEC-6 | A fim de evitar a usurpação de identidade ou a criação de utilizadores falsos, o servidor deve autenticar a aplicação. |
| SEC-7 | A aplicação deve autenticar o servidor central. |
| SEC-8 | As funcionalidades do servidor devem ser protegidas contra ataques de repetição. |
| SEC-9 | As informações transmitidas pelo servidor central devem ser assinadas para autenticar a sua origem e integridade. |
| SEC-10 | O acesso a todos os dados armazenados no servidor central e não disponibilizados ao público deve ser reservado apenas a pessoas autorizadas. |
| SEC-11 | O gestor de permissões do dispositivo a nível do sistema operativo só deve solicitar as permissões necessárias para aceder e utilizar, quando necessário, os módulos de comunicação, armazenar os dados no terminal e trocar informações com o servidor central. |

## 9. Proteção de dados pessoais e da privacidade das pessoas singulares

*Aviso: as diretrizes a seguir apresentadas dizem respeito a uma aplicação cuja única finalidade é o rastreio de contactos.*

| | |
|---|---|
| PRIV-1 | Os intercâmbios de dados devem respeitar a privacidade dos utilizadores (e, nomeadamente, respeitar o princípio da minimização de dados). |
| PRIV-2 | A aplicação não deve permitir que os utilizadores, ao utilizá-la, sejam identificados diretamente. |
| PRIV-3 | A aplicação não deve permitir que os movimentos dos utilizadores sejam rastreados. |
| PRIV-4 | A utilização da aplicação não deve permitir que os utilizadores infiram quaisquer informações sobre outros utilizadores (especialmente sobre se são ou não portadores do vírus). |
| PRIV-5 | A confiança no servidor central deve ser limitada. A gestão do servidor central deve seguir regras de governação claramente definidas e incluir todas as medidas necessárias para garantir a sua segurança. A localização do servidor central deve permitir uma supervisão eficaz por parte da autoridade de supervisão competente. |
| PRIV-6 | Deve ser realizada, e tornada pública, uma avaliação de impacto sobre a proteção de dados. |
| PRIV-7 | A aplicação só deve revelar ao utilizador se o mesmo foi exposto ao vírus e, se possível, sem revelar informações sobre outros utilizadores, o número de vezes e as datas em que a exposição terá ocorrido. |
| PRIV-8 | As informações veiculadas pela aplicação não devem permitir que os utilizadores identifiquem os utilizadores portadores do vírus, nem os seus movimentos. |
| PRIV-9 | As informações veiculadas pela aplicação não devem permitir que as autoridades de saúde identifiquem utilizadores que tenham sido potencialmente expostos sem o seu consentimento. |
| PRIV-10 | As solicitações feitas pela aplicação ao servidor central não devem revelar nada sobre o portador de vírus. |
| PRIV-11 | As solicitações feitas pela aplicação ao servidor central não devem revelar quaisquer informações desnecessárias sobre o utilizador, exceto, possivelmente, e somente quando necessário, no que se refere ao seu identificador pseudonimizado e à sua lista de contactos. |
| PRIV-12 | Os ataques de ligação não devem ser possíveis. |
| PRIV-13 | Os utilizadores devem poder exercer os seus direitos através da aplicação. |
| PRIV-14 | A desinstalação da aplicação deve resultar na eliminação de todos os dados recolhidos localmente. |
| PRIV-15 | A aplicação só deve recolher dados transmitidos por instâncias da aplicação ou por aplicações equivalentes interoperáveis. Não devem ser recolhidos quaisquer dados relativos a outras aplicações e/ou dispositivos de comunicação de proximidade. |

| | |
|---|---|
| PRIV-16 | A fim de evitar a reidentificação pelo servidor central, devem ser implementados servidores intermediários. O objetivo destes *servidores não coniventes («non-colluding») consiste em* misturar os identificadores de vários utilizadores (tanto os de portadores de vírus como os enviados pelos requerentes) antes de os partilhar com o servidor central, de modo a evitar que o servidor central conheça os identificadores (como, por exemplo, os endereços IP) dos utilizadores. |
| PRIV-17 | A aplicação e o servidor devem ser cuidadosamente desenvolvidos e configurados para não recolherem dados desnecessários (por exemplo, não devem ser incluídos identificadores nos registos do servidor, etc.) e para impedir a utilização de qualquer SDK (*Kit* de desenvolvimento de programas informáticos) de terceiros que recolha dados para outras finalidades. |

A maioria das aplicações de rastreio de contactos que são atualmente objeto de debate seguem basicamente duas abordagens quando um utilizador é declarado como estando infetado: podem enviar para um servidor o histórico de contactos de proximidade obtido através do procedimento de digitalização, ou podem enviar a lista dos seus próprios identificadores transmitidos. Os princípios a seguir apresentados são rejeitados em função destas duas abordagens. Embora estas sejam as abordagens aqui debatidas, tal não significa que não sejam possíveis, ou mesmo preferíveis, outras abordagens como, por exemplo, abordagens que implementem alguma forma de cifragem de ponta a ponta ou que utilizem outras tecnologias de reforço da segurança ou da privacidade.

**9.1. Princípios aplicáveis** apenas **quando a aplicação envia uma lista de contactos para o servidor:**

| | |
|---|---|
| CON-1 | O servidor central deve recolher o histórico de contactos dos utilizadores identificados como tendo sido testados e o resultado ter sido positivo para SARS-CoV-2 como resultado de ações voluntárias da sua parte. |
| CON-2 | O servidor central não deve manter nem fazer circular uma lista dos identificadores pseudonimizados dos utilizadores portadores do vírus. |
| CON-3 | O histórico de contactos armazenado no servidor central deve ser apagado assim que os utilizadores forem notificados da sua proximidade com uma pessoa diagnosticada como estando infetada. |
| CON-4 | Nenhuma informação deve sair do equipamento do utilizador, salvo quando um utilizador detetado como estando infetado partilha o seu histórico de contactos com o servidor central ou quando um utilizador apresenta um pedido ao servidor no sentido de descobrir a sua potencial exposição ao vírus. |
| CON-5 | Qualquer identificador incluído no histórico local deve ser eliminado após X dias contados a partir da data da sua recolha (sendo o valor X definido pelas autoridades de saúde). |
| CON-6 | Os históricos de contactos apresentados por utilizadores diferentes não devem ser objeto de tratamento posterior, por exemplo, para a criação de mapas de proximidade globais. |
| CON-7 | Os dados contidos nos registos do servidor devem ser minimizados e devem cumprir os requisitos em matéria de proteção de dados. |

**9.2. Princípios aplicáveis apenas quando a aplicação envia uma lista dos seus próprios identificadores para o servidor:**

| | |
|---|---|
| ID-1 | O servidor central deve recolher os identificadores transmitidos pela aplicação dos utilizadores identificados como tendo sido testados e o resultado ter sido positivo para SARS-CoV-2 como resultado de ações voluntárias da sua parte. |
| ID-2 | O servidor central não deve manter nem fazer circular o histórico de contactos dos utilizadores portadores do vírus. |
| ID-3 | Os identificadores armazenados no servidor central devem ser eliminados assim que forem distribuídos às outras aplicações. |
| ID-4 | Nenhuma informação deve sair do equipamento do utilizador, salvo quando um utilizador detetado como estando infetado partilha os seus identificadores com o servidor central ou quando um utilizador apresenta um pedido ao servidor no sentido de descobrir a sua potencial exposição ao vírus. |
| ID-5 | Os dados contidos nos registos do servidor devem ser minimizados e devem cumprir os requisitos em matéria de proteção de dados. |