Manual de Procedimentos para Notificar a CNPD por

Violação de Dados Pessoais

(Data Breach)

INTRODUÇÃO

O Regulamento Geral sobre a Proteção de Dados (RGPD) introduz o requisito de que seja notificada a violação de dados pessoais (a seguir «violação») à autoridade de controlo nacional competente[1] (ou, no caso de uma violação transfronteiriça, à autoridade principal) e, em certos casos, de comunicar a violação às pessoas singulares cujos dados pessoais tenham sido afetados pela violação.

I. Notificação da violação de dados pessoais ao abrigo do RGPD

A. Considerações básicas de segurança

Um dos requisitos do RGPD é que, através da adoção de medidas técnicas e organizativas adequadas, os dados pessoais sejam tratados, por forma a assegurar a segurança adequada dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental[2].

Por conseguinte, o RGPD exige que tanto os responsáveis pelo tratamento como os subcontratantes apliquem medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco imposto aos dados pessoais que estão a ser tratados. Devem ter em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco decorrente do tratamento, cuja probabilidade e gravidade podem ser variáveis, para os direitos e liberdades das pessoas singulares[3]. Além disso, o RGPD exige que sejam adotadas todas as medidas tecnológicas de proteção e de organização adequadas para apurar imediatamente a ocorrência de uma violação, o que determina se está envolvida a obrigação de notificação[4].

Por conseguinte, um elemento fundamental de qualquer política em matéria de segurança de dados é conseguir, sempre que possível, prevenir uma violação e, quando esta aconteça, dar uma resposta em tempo útil.

---

[1] Ver artigo 4.º, ponto 21, do RGPD

[2] Ver artigo 5.º, n.º 1, alínea f) e artigo 32.º.

[3] Artigo 32.º; ver igualmente o considerando 83.

[4] Ver considerando 87.

B. Em que consiste uma violação de dados pessoais?

1. Definição

Em qualquer tentativa de resolver uma violação, o responsável pelo tratamento deve primeiro ser capaz de reconhecer uma. O RGPD define «violação de dados pessoais» no artigo 4.º, n.º 12, como:

«[...] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento».

O que se entende por «destruição» de dados pessoais deve ser bem claro: refere-se aos dados que deixam de existir, ou deixam de existir num formato que seja de alguma utilidade para o responsável pelo tratamento. O significado de «dano» também deve ser relativamente claro: trata-se dos dados pessoais que foram alterados, corrompidos, ou já não estão completos. Em termos de «perda» de dados pessoais, tal deve ser interpretado como os dados ainda poderem existir, mas o responsável pelo tratamento perdeu o controlo ou o acesso a eles, ou já não os tem em sua posse. Por último, o tratamento não autorizado ou ilícito pode incluir a divulgação de dados pessoais a (ou o acesso por) destinatários que não estão autorizados a receber (ou a aceder) os dados, ou qualquer outra forma de tratamento que viole o RGPD.

O que deve ficar claro é que uma violação é um tipo de incidente de segurança. No entanto, como indicado pelo artigo 4.º, n.º 12, o RGPD só é aplicável quando existe uma violação de *dados pessoais*. A consequência de tal violação é que o responsável pelo tratamento não poderá assegurar o cumprimento dos princípios relativos ao tratamento de dados pessoais, conforme definido no artigo 5.º do RGPD. Isto realça a diferença entre um incidente de segurança e uma violação de dados pessoais – em essência, enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais[5]. Os potenciais efeitos adversos de uma violação sobre as pessoas singulares são analisados abaixo.

[5] Deve notar-se que um incidente de segurança não se limita a modelos de ameaça em que é efetuado um ataque a uma organização por parte de uma fonte externa, mas inclui incidentes decorrentes do tratamento interno que violam os princípios de segurança.

2. Tipos de violações de dados pessoais

No seu Parecer 03/2014, relativo à notificação de violação, o GT29 explicou que as violações podem ser categorizadas de acordo com os três princípios bem conhecidos de segurança da informação que se seguem[6]:

- «Violação da confidencialidade» - quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.

- «Violação da integridade» - quando existe uma alteração acidental ou não autorizada dos dados pessoais.

- «Violação da disponibilidade» - quando existe uma perda de acesso ou a destruição acidental ou não autorizada[7] de dados pessoais.

Importa igualmente notar que, dependendo das circunstâncias, uma violação pode dizer respeito à confidencialidade, à integridade e à disponibilidade de dados pessoais simultaneamente, assim como a qualquer combinação destas.

Enquanto determinar se existiu uma violação da confidencialidade ou da integridade é relativamente claro, determinar a ocorrência de uma violação da disponibilidade pode ser menos óbvio. Uma violação será sempre considerada uma violação da disponibilidade, se tiver ocorrido uma perda permanente ou uma destruição de dados pessoais.

Exemplos de uma perda de disponibilidade: dados que foram apagados acidentalmente ou por uma pessoa não autorizada ou, no caso de dados cifrados de forma segura, a perda da chave de decifração. Caso o responsável pelo tratamento não consiga restaurar o acesso aos dados, por

---

[6] Ver Parecer 03/2014.

[7] É um facto que o «acesso» é uma parte fundamental da «disponibilidade». Ver, por exemplo, NIST SP80053rev4, que define «disponibilidade» como: «Assegurar o acesso atempado e fiável e a utilização de informação», disponível em http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. O CNSSI-4009 também se refere à: «Acesso atempado e fiável a dados e serviços de informação para utilizadores autorizados.» Ver https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. A ISO/IEC 27000:2016 também define «disponibilidade» como a «Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada»: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

exemplo, a partir de uma cópia de segurança, tal é considerado uma perda permanente de disponibilidade.

Uma perda de disponibilidade também pode ocorrer quando tiver havido uma interrupção significativa do serviço normal de uma organização, por exemplo, uma falha de energia ou um ataque de negação de serviço, que torne os dados pessoais indisponíveis.

Pode colocar-se a questão de saber se uma perda temporária de disponibilidade dos dados pessoais deve ser considerada uma violação e, em caso afirmativo, se deve ser notificada. O artigo 32.º do RGPD, «segurança do tratamento», explica que ao aplicar medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco, deve ter-se em conta, nomeadamente, a «[a] capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento» e «[a] capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico».

Por conseguinte, um incidente de segurança que resulte na indisponibilidade dos dados pessoais por um período de tempo também é um tipo de violação, uma vez que a falta de acesso aos dados pode ter um impacto significativo sobre os direitos e liberdades das pessoas singulares. Para que fique claro, quando os dados pessoais estão indisponíveis devido à realização de uma manutenção dos sistemas, isso não é uma «violação da segurança», conforme definida no artigo 4.º, n.º 12.

Tal como acontece com a perda permanente ou a destruição de dados pessoais (ou, de facto, qualquer outro tipo de violação), uma violação que envolva a perda temporária de disponibilidade deve ser documentada de acordo com o artigo 33.º, n.º 5. Isso ajuda o responsável pelo tratamento a demonstrar responsabilidade perante a autoridade de controlo, que pode pedir para ver esses registos[8]. No entanto, dependendo das circunstâncias da violação, esta pode ou não exigir a notificação à autoridade de controlo e comunicação às pessoas afetadas. O responsável pelo tratamento necessitará de avaliar a probabilidade e a gravidade do impacto sobre os direitos e liberdades das pessoas singulares resultantes da falta de disponibilidade dos dados pessoais. De acordo com o artigo 33.º, o responsável pelo tratamento deverá proceder à notificação, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. É evidente que será necessário analisar cada caso.

[8] Ver artigo 33.º, n.º 5.

É de salientar que, embora a perda de disponibilidade dos sistemas de um responsável pelo tratamento possa ser apenas temporária e não ter impacto sobre as pessoas, é importante que o responsável pelo tratamento tenha em conta todas as possíveis consequências de uma violação, uma vez que esta pode exigir notificação por outras razões.

Por exemplo, a infeção por software de sequestro (software malicioso que cifra os dados do responsável pelo tratamento até que seja pago um resgate) pode levar a uma perda temporária de disponibilidade, se os dados puderem ser restaurados a partir de uma cópia de segurança. Contudo, a intrusão na rede ocorreu e pode ser exigida notificação, se o incidente for classificado como uma violação da confidencialidade (ou seja, os dados pessoais forem acedidos pelo atacante) e isto representar um risco para os direitos e liberdades das pessoas.

3. Possíveis consequências de uma violação dos dados pessoais

Uma violação pode potencialmente ter um leque de efeitos adversos significativos sobre as pessoas, que podem resultar em danos físicos, materiais ou imateriais. O RGPD explica que estes podem incluir a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação e a perda de confidencialidade de dados pessoais protegidos por sigilo profissional. Podem incluir igualmente qualquer outra desvantagem económica ou social significativa para essas pessoas singulares[9].

Assim, o RGPD exige que o responsável pelo tratamento notifique a violação à autoridade de controlo competente, a menos que seja improvável que resulte no risco de tais efeitos adversos ocorrerem. Quando existe um risco elevado de ocorrência destes efeitos adversos, o RGPD exige que o responsável pelo tratamento comunique a violação às pessoas singulares afetadas logo que seja razoavelmente possível[10].

A importância de ser capaz de identificar uma violação, avaliar o risco para as pessoas e, então, proceder à notificação, se necessário, é salientada no considerando 87 do RGPD.

«Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar

[9] Ver também os considerandos 85 e 75.
[10] Ver igualmente o considerando 86.

rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.»

São consideradas na secção IV outras orientações sobre a avaliação do risco de efeitos adversos para as pessoas.

Se os responsáveis pelo tratamento não notificarem a autoridade de controlo ou os titulares dos dados de uma violação de dados, ou ambos, mesmo que os requisitos do artigo 33.º e/ou 34.º sejam cumpridos, é colocada à autoridade de controlo uma escolha que deve incluir a análise de todas as medidas corretivas à sua disposição, incluindo a imposição de uma coima adequada[11], quer acompanhada de uma medida corretiva nos termos do artigo 58.º, n.º 2, quer por si própria. Caso se opte por uma coima, o seu valor pode ser até 10 000 000 EUR ou até 2 % do volume de negócios anual a nível mundial, de uma empresa de acordo com o artigo 83.º, n.º 4, alínea a), do RGPD. É igualmente importante ter em mente que, em certos casos, a não notificação de uma violação pode revelar uma ausência de medidas de segurança ou uma inadequação das medidas de segurança existentes. As orientações do GT29 relativas às coimas estabelecem o seguinte: «A ocorrência de várias infrações distintas, cometidas em conjunto em qualquer caso individual específico, significa que a autoridade de controlo pode aplicar as coimas a um nível que seja efetivo, proporcionado e dissuasivo, dentro do limite aplicável à infração mais grave.» Nesse caso, a autoridade de controlo terá também a possibilidade de emitir sanções, por um lado, por falta de notificação ou de comunicação da violação (artigos 33.º e 34.º) e, por outro, por ausência de medidas (adequadas) de segurança (artigo 32.º), uma vez que se trata de duas infrações separadas.

[11] Para informações mais pormenorizadas, ver as orientações do GT29 sobre a aplicação e a fixação do valor das coimas, disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

II. Artigo 33.º - Notificação à autoridade de controlo

A. Quando notificar

1. Requisitos do artigo 33.º

«Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.»

O considerando 87 estabelece[12] o seguinte:

«Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.»

2. Quando é que um responsável pelo tratamento tem «conhecimento»? Conforme pormenorizado acima, o RGPD exige que, em caso de violação, o responsável pelo tratamento notifique a violação sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma. Isto pode levantar a questão de saber quando é que se pode considerar que um responsável pelo tratamento teve «conhecimento» da violação. O GT29 considera que se deve considerar que um responsável pelo tratamento tem «conhecimento» quando tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais.

[12] O considerando 85 também é importante neste caso.

No entanto, conforme indicado anteriormente, o RGPD exige que o responsável pelo tratamento aplique todas as medidas técnicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação e para informar rapidamente a autoridade de controlo e os titulares dos dados. Estabelece igualmente que, para comprovar que a notificação foi enviada sem demora injustificada, importa ter em conta, em especial, a natureza e a gravidade da violação e as respetivas consequências e efeitos adversos para o titular dos dados[13]. O responsável pelo tratamento fica assim obrigado a assegurar que este tenha «conhecimento» de eventuais violações em tempo útil, para que possa tomar medidas adequadas.

As circunstâncias de uma violação irão ditar as condições exatas em que se pode considerar que um responsável pelo tratamento tem «conhecimento» dessa violação. Nalguns casos, será relativamente claro desde o início se ocorreu uma violação, ao passo que noutros poderá ser necessário algum tempo para apurar se foram afetados dados pessoais. No entanto, a ênfase deve estar na ação imediata para investigar um incidente, a fim de determinar se os dados pessoais foram de facto violados e, em caso afirmativo, tomar medidas de reparação e notificar, se necessário.

Exemplos:

- No caso de perda de uma "pen" ou outro suporte de dados externo com dados pessoais não encriptados, muitas vezes não é possível determinar se houve acesso de pessoas não autorizadas a esses dados. Contudo, mesmo que o responsável pelo tratamento não consiga determinar se ocorreu uma violação da confidencialidade esse caso tem de ser notificado, uma vez que existe um grau razoável de certeza de que ocorreu uma violação da disponibilidade; o responsável pelo tratamento teria tomado «conhecimento» ao aperceber-se da perda da "pen" USB.

- Um terceiro informa um responsável pelo tratamento de que recebeu acidentalmente os dados pessoais de um dos seus clientes e fornece elementos de prova da divulgação não autorizada. Uma vez apresentadas provas de uma violação da confidencialidade ao responsável pelo tratamento, não podem existir dúvidas de que este tomou «conhecimento».

[13] Ver considerando 87.

- Um responsável pelo tratamento deteta uma eventual intrusão na sua rede. Verifica os seus sistemas para apurar se os dados pessoais contidos nesse sistema foram afetados e confirma ser esse o caso. Mais uma vez, dado que o responsável pelo tratamento possui agora provas inequívocas de uma violação, não podem existir dúvidas de que este tomou «conhecimento».

- Um cibercriminoso contacta o responsável pelo tratamento para pedir um resgate após ter pirateado o seu sistema. Nesse caso, após ter verificado o seu sistema para confirmar que foi pirateado, o responsável pelo tratamento possui provas inequívocas de que ocorreu uma violação, pelo que existem dúvidas de que tomou conhecimento.

Após ter sido informado de uma potencial violação por um indivíduo, uma organização de comunicação ou outra fonte, ou ao detetar ele próprio um incidente de segurança, o responsável pelo tratamento pode realizar um curto período de investigação para apurar se ocorreu ou não uma violação. Durante este período de investigação o responsável pelo tratamento não deve ser considerado como tendo «conhecimento». No entanto, é expectável que a investigação inicial comece o mais rapidamente possível, para apurar, com razoável grau de certeza, a ocorrência de uma violação; pode seguir-se uma investigação mais aprofundada.

Assim que o responsável pelo tratamento tenha tomado conhecimento, uma violação notificável deve ser notificada sem demora injustificada, e sempre que possível, até 72 horas. Durante este período, o responsável pelo tratamento deve avaliar o risco provável para as pessoas, a fim de determinar se o requisito de notificação foi acionado, bem como as medidas necessárias para abordar a violação. No entanto, um responsável pelo tratamento pode já ter uma avaliação inicial do risco potencial, que pode resultar de uma violação, no âmbito de uma avaliação de impacto sobre a proteção de dados (AIPD)[14] feita antes da operação de tratamento em causa. Contudo, a AIPD pode ser mais generalizada em comparação com as circunstâncias específicas de qualquer violação real e, assim, em qualquer caso, deverá ser realizada uma avaliação adicional que tenha em conta essas circunstâncias. Para mais pormenores sobre a avaliação do risco, ver a secção IV.

Na maioria dos casos, estas medidas preliminares devem estar concluídas logo após o alerta inicial (ou seja, quando o responsável pelo tratamento ou subcontratante suspeita da ocorrência de um incidente de segurança que pode envolver dados pessoais) – só deve demorar mais em casos excecionais.

[14] Ver as orientações do GT29 sobre as AIPD aqui: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Exemplo:

- Um indivíduo informa o responsável pelo tratamento de que recebeu uma mensagem de correio eletrónico a fazer-se passar pelo responsável pelo tratamento relativamente à sua (real) utilização do serviço deste, sugerindo que a segurança do responsável pelo tratamento foi comprometida. O responsável pelo tratamento conduz um curto período de investigação e identifica uma intrusão na sua rede, bem como provas de acesso não autorizado aos dados pessoais. Seria agora considerado como tendo «conhecimento», sendo exigida a notificação à autoridade de controlo, a menos que seja pouco provável que represente um risco para os direitos e liberdades das pessoas. O responsável pelo tratamento deve tomar medidas de reparação para fazer face à violação.

Por conseguinte, deve possuir processos internos para ser capaz de detetar e fazer face a uma violação. Por exemplo, para encontrar algumas irregularidades no tratamento de dados, o responsável pelo tratamento ou subcontratante pode utilizar certas medidas técnicas, como o fluxo de dados e analisadores de registos, a partir dos quais é possível definir eventos e alertas através da correlação de quaisquer dados de registo[15]. Quando uma violação é detetada, é importante que seja comunicada aos níveis superiores competentes, para que possa ser reparada e, se for caso disso, notificada em conformidade com o artigo 33.º e, se necessário, com o artigo 34.º. Tais medidas e mecanismos de comunicação podem ser pormenorizados nos planos de resposta a incidentes do responsável pelo tratamento e/ou mecanismos de governação. Estes vão ajudar o responsável pelo tratamento a planear de maneira eficaz e a determinar quem detém a responsabilidade operacional dentro da organização para gerir uma violação e como fazer face ou não a um incidente, se necessário.

O responsável pelo tratamento deve também possuir acordos com quaisquer subcontratantes a que recorra, que também têm a obrigação de notificar o responsável pelo tratamento no caso de uma violação (ver abaixo).

Embora seja da responsabilidade dos responsáveis pelo tratamento e dos subcontratantes adotar medidas adequadas para prevenir, dar resposta e fazer face a uma violação, existem algumas medidas práticas que devem ser tomadas em todos os casos.

[15] Importa notar que os dados de registo que facilitam a realização de auditorias, por exemplo, sobre o armazenamento, alterações ou apagamento de dados, podem também ser considerados dados pessoais relativos à pessoa que iniciou a respetiva operação de tratamento.

- As informações relativas a todos os eventos relacionados com segurança devem ser dirigidas à pessoa ou pessoas responsáveis com a tarefa de responder a incidentes, apurar a existência de uma violação e avaliar o risco.
- Os riscos para as pessoas resultantes de uma violação devem, pois, ser avaliados (probabilidade de nenhum risco, de risco ou de risco elevado), com secções relevantes da organização a serem informadas.
- Se necessário, deve-se notificar a autoridade de controlo e comunicar eventualmente a violação às pessoas afetadas.
- Simultaneamente, o responsável pelo tratamento deve agir para conter e reparar a violação.
- A documentação da violação deve ocorrer à medida que esta se desenvolve.

Por conseguinte, deve ficar claro que existe a obrigação de o responsável pelo tratamento responder a qualquer alerta inicial e apurar se ocorreu, de facto, uma violação. Este breve período permite levar a cabo uma investigação e que o responsável pelo tratamento recolha provas e outros pormenores relevantes. No entanto, assim que o responsável pelo tratamento tiver estabelecido com um grau razoável de certeza que ocorreu uma violação, se as condições do artigo 33.º, n.º 1, estiverem preenchidas, deve notificar a autoridade de controlo sem demora injustificada e, se possível, no prazo de 72 horas[16]. Se o responsável pelo tratamento não agir em tempo útil e se tornar evidente que ocorreu uma violação, tal pode ser considerado uma não notificação nos termos do artigo 33.º.

O artigo 32.º clarifica que o responsável pelo tratamento e o subcontratante devem adotar medidas técnicas e organizativas adequadas para assegurar um nível adequado de segurança dos dados pessoais: a capacidade de detetar, de dar resposta e de comunicar uma violação em tempo útil deve ser encarada como um elemento essencial destas medidas.

[16] Ver Regulamento n.º 1182/71, relativo à determinação das regras aplicáveis aos prazos, às datas e aos termos, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31971R1182&from=PT

3. Responsáveis conjuntos pelo tratamento

O artigo 26.º diz respeito aos responsáveis conjuntos pelo tratamento e especifica que os responsáveis conjuntos devem determinar as respetivas responsabilidades pelo cumprimento do RGPD[17]. Tal inclui determinar que parte terá responsabilidade pelo cumprimento das obrigações previstas nos artigos 33.º e 34.º. O GT29 recomenda que os acordos contratuais entre responsáveis conjuntos incluam disposições que determinem que responsável pelo tratamento assumirá a liderança ou será responsável pelo cumprimento das obrigações de notificação de violação do RGPD.

4. Obrigações do subcontratante

O responsável pelo tratamento detém a responsabilidade global pela proteção dos dados pessoais, mas o subcontratante desempenha um papel importante para que o responsável pelo tratamento consiga cumprir as suas obrigações; e isto inclui a notificação de violação. De facto, o artigo 28.º, n.º 3, especifica que o tratamento em subcontratação deve ser regulado por um contrato ou por outro ato normativo. O artigo 28.º, n.º 3, alínea f), estabelece que o contrato ou outro ato normativo deve estipular que o subcontratante «[p]resta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante».

O artigo 33.º, n.º 2, esclarece que, se um responsável pelo tratamento recorrer a um subcontratante e este tomar conhecimento de uma violação dos dados pessoais que está a tratar em nome do responsável pelo tratamento, deve notificar o responsável pelo tratamento «sem demora injustificada». É de salientar que o subcontratante não necessita de avaliar primeiro a probabilidade de risco resultante de uma violação antes de notificar o responsável pelo tratamento; cabe ao responsável pelo tratamento efetuar essa avaliação ao ter conhecimento da violação. O subcontratante só necessita de apurar a ocorrência de uma violação e notificá-la ao responsável pelo tratamento. O responsável pelo tratamento recorre ao subcontratante para alcançar os seus objetivos; por conseguinte, em princípio, considera-se que o responsável pelo tratamento tomou «conhecimento» assim que o subcontratante o informa da violação. A obrigação de o subcontratante notificar o seu responsável pelo tratamento permite ao responsável pelo tratamento responder a uma violação e determinar se é ou não exigido notificar a autoridade de controlo em conformidade com o artigo 33.º, n.º 1, e as pessoas afetadas em conformidade com o artigo 34.º, n.º 1. O responsável pelo tratamento também pode querer investigar a

[17] Ver igualmente o considerando 79.

violação, uma vez que o subcontratante pode não estar em posição de saber todos os fatos relevantes relacionados com o assunto, por exemplo, se uma cópia ou cópia de segurança dos dados pessoais destruídos ou perdidos pelo subcontratante ainda se encontra na posse do responsável pelo tratamento. Tal pode ditar a necessidade de o responsável pelo tratamento proceder ou não à notificação.

O RGPD não prevê um prazo limite explícito para o subcontratante alertar o responsável pelo tratamento, apenas que o deve fazer «sem demora injustificada». Por conseguinte, o GT29 recomenda que o subcontratante notifique imediatamente o responsável pelo tratamento, fornecendo informações adicionais sobre a violação por fases à medida que os pormenores se tornam disponíveis. Isto é importante para ajudar o responsável pelo tratamento a cumprir o requisito de notificação à autoridade de controlo no prazo de 72 horas.

Conforme explicado acima, o contrato entre o responsável pelo tratamento e o subcontratante deve especificar como cumprir os requisitos expressos no artigo 33.º, n.º 2, além de outras disposições do RGPD. Isto pode incluir requisitos de notificação precoce por parte do subcontratante, que, por sua vez, apoiam as obrigações do responsável pelo tratamento de informar a autoridade de controlo no prazo de 72 horas.

Sempre que o subcontratante presta serviços a vários responsáveis pelo tratamento que são todos afetados pelo mesmo incidente, o subcontratante terá de comunicar pormenores do incidente a cada um dos responsáveis pelo tratamento.

Um subcontratante pode fazer uma notificação em nome do responsável pelo tratamento, se este lhe tiver dado a autorização adequada e isto fizer parte do acordo contratual entre responsável pelo tratamento e subcontratante. A notificação deve ser efetuada em conformidade com os artigos 33.º e 34.º. No entanto, importa salientar que a responsabilidade jurídica de notificar continua a ser do responsável pelo tratamento.

B. Prestação de informações à autoridade de controlo

1. Informações a comunicar

Quando um responsável pelo tratamento notifica uma violação à autoridade de controlo, o artigo 33.º, n.º 3, prevê que, no mínimo, deve:

a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

c) Descrever as consequências prováveis da violação de dados pessoais;

d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos».

O RGPD não define categorias de titulares de dados ou de registos de dados pessoais. No entanto, o GT29 sugere que as categorias de titulares de dados digam respeito aos vários tipos de pessoas singulares cujos dados pessoais foram afetados por uma violação: dependendo dos descritores utilizados, pode incluir, entre outros, crianças e outros grupos vulneráveis, pessoas com deficiência, trabalhadores ou clientes. De igual modo, as categorias de registos de dados pessoais podem referir-se a diferentes tipos de registos que o responsável pelo tratamento pode tratar, como dados relativos à saúde, registos escolares, informação relativa à ação social, dados financeiros, números de contas bancárias, números de passaporte, etc.

O considerando 85 esclarece que um dos objetivos da notificação consiste em limitar os danos para as pessoas singulares. Assim, se os tipos de titulares de dados ou os tipos de dados pessoais indicarem um risco de dano específico decorrente de uma violação (por exemplo, roubo de identidade, fraude, perdas financeiras, ameaça ao sigilo profissional), então, é importante que a notificação indique estas categorias. Desta forma, está ligada ao requisito de descrição das consequências prováveis da violação.

Quando não estiverem disponíveis informações exatas (por exemplo, o número exato de titulares dos dados afetados), tal não deve ser um obstáculo à notificação atempada da violação. O RGPD permite que sejam feitas aproximações quanto ao número de pessoas afetadas e ao número de registos de dados pessoais em causa. É mais importante atenuar os efeitos adversos da violação do que fornecer números precisos. Deste modo, quando se torna evidente que ocorreu uma violação, mas a sua dimensão ainda não é conhecida, uma notificação por fases (ver abaixo) é uma maneira segura de cumprir as obrigações de notificação.

O artigo 33.º, n.º 3, estabelece que um responsável pelo tratamento «deve, pelo menos» prestar esta informação com uma notificação, para que o responsável pelo tratamento possa, se necessário, optar por fornecer pormenores adicionais. Diferentes tipos de violações (confidencialidade, integridade ou disponibilidade) podem exigir que seja fornecida informação adicional de modo a explicar plenamente as circunstâncias de cada caso.

Como parte da sua notificação à autoridade de controlo, um responsável pelo tratamento pode considerar útil nomear o seu subcontratante, se ele for a principal causa da violação, especialmente se isso tiver levado a um incidente que afeta os registos de dados pessoais de muitos outros responsáveis pelo tratamento que recorrem ao mesmo subcontratante.

De qualquer forma, a autoridade de controlo pode solicitar mais informações no âmbito da sua investigação a uma violação.

2. Notificação por fases

Dependendo da natureza da violação, pode ser necessária investigação adicional por parte do responsável pelo tratamento, para apurar todos os factos relevantes relacionados com o incidente. O artigo 33.º, n.º 4, prevê o seguinte:

«Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.»

Isto significa que o RGPD reconhece que os responsáveis pelo tratamento nem sempre estarão na posse de todas as informações necessárias relativas a uma violação no prazo de 72 horas após terem tido conhecimento da mesma, uma vez que podem não estar disponíveis durante o período inicial

pormenores completos e abrangentes do incidente. Assim sendo, permite uma notificação por fases. É mais provável que esse seja o caso de violações mais complexas, como alguns tipos de incidentes de cibersegurança em que, por exemplo, possa ser necessária uma investigação forense aprofundada para determinar plenamente a natureza da violação e em que medida os dados pessoais foram afetados. Por conseguinte, em muitos casos, o responsável pelo tratamento terá de proceder a uma investigação e um acompanhamento mais aprofundados, com informação suplementar num momento posterior. Tal é admissível, desde que o responsável pelo tratamento justifique o seu atraso, nos termos do artigo 33.º, n.º 1. O GT29 recomenda que, quando um responsável pelo tratamento notificar inicialmente a autoridade de controlo, também informe a mesma se ainda não possuir todas as informações necessárias e forneça mais pormenores posteriormente. A autoridade de controlo deve acordar como e quando deve ser fornecida a informação suplementar. Tal não impede que o responsável pelo tratamento forneça informação suplementar em qualquer outra fase, se tiver conhecimento de informações adicionais relevantes acerca da violação que devam ser fornecidos à autoridade de controlo.

O requisito de notificação visa encorajar os responsáveis pelo tratamento a agir rapidamente em caso de violação, contê-la e, se possível, recuperar os dados pessoais afetados, e procurar o aconselhamento relevante da autoridade de controlo. Notificar a autoridade de controlo nas primeiras 72 horas pode permitir ao responsável pelo tratamento certificar-se de que as decisões sobre notificar ou não notificar as pessoas singulares estão corretas.

No entanto, o objetivo de notificar a autoridade de controlo não consiste apenas em obter orientações sobre a notificação das pessoas singulares afetadas. Em alguns casos, será óbvio que, devido à natureza da violação e à gravidade do risco, o responsável pelo tratamento terá de notificar as pessoas afetadas sem demora. Por exemplo, se existir uma ameaça imediata de roubo de identidade, ou se categorias especiais de dados pessoais[18] forem divulgadas em linha, o responsável pelo tratamento deve agir sem demora injustificada para conter a violação e comunicá-la às pessoas em causa (ver secção III). Em circunstâncias excecionais, isto pode mesmo acontecer antes da notificação à autoridade de controlo. De um modo mais geral, a notificação à autoridade de controlo não pode servir de justificação para não comunicar a violação ao titular dos dados, quando tal é exigido.

[18] Ver artigo 9.º.

Deve também ficar claro que, após efetuar uma notificação inicial, o responsável pelo tratamento pode facultar informações atualizadas à autoridade de controlo, se uma investigação subsequente revelar provas de que o incidente de segurança foi contido e não ocorreu uma violação. Esta informação pode depois ser acrescentada à informação já fornecida à autoridade de controlo e o incidente registado em conformidade como não se tratando de uma violação. Não existe uma sanção por comunicar um incidente que, em última análise, não é uma violação.

Por exemplo, um responsável pelo tratamento notifica a autoridade de controlo no prazo de 72 horas após ter detetado uma violação de que perdeu a "pen" USB que contém uma cópia dos dados pessoais de alguns dos seus clientes. A "pen" USB é posteriormente encontrada mal arquivada nas instalações do responsável pelo tratamento e recuperada. O responsável pelo tratamento atualiza a autoridade de controlo e solicita que a notificação seja alterada.

É de salientar que uma abordagem faseada da notificação já existe ao abrigo das obrigações aplicáveis da Diretiva 2002/58/CE e do Regulamento (UE) n.º 611/2013, e de outros incidentes comunicados pelo próprio.

3. Notificações atrasadas

O artigo 33.º, n.º 1, esclarece que, se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, deve ser acompanhada dos motivos do atraso. Isto, juntamente com o conceito de notificação por fases, leva a reconhecer que o responsável pelo tratamento nem sempre pode ser capaz de notificar uma violação dentro desse prazo, e que pode ser admissível uma notificação atrasada.

Tal cenário pode ocorrer se, por exemplo, um responsável pelo tratamento for alvo de várias violações de confidencialidade semelhantes num curto período de tempo, que afetem um grande número de titulares de dados da mesma maneira. Um responsável pelo tratamento podia ter conhecimento de uma violação e, ao iniciar a sua investigação, e antes da notificação, detetar outras violações semelhantes com causas diferentes. Dependendo das circunstâncias, o responsável pelo tratamento pode demorar algum tempo a apurar a dimensão das violações e, em vez de notificar cada uma das violações individualmente, pode organizar uma notificação útil, que represente várias violações muito semelhantes, com causas possíveis diferentes. Isso pode levar a que a notificação à autoridade de controlo se atrase por mais de 72 horas após o responsável pelo tratamento ter tido conhecimento dessas violações.

Em rigor, cada violação individual é um incidente cuja comunicação é obrigatória. No entanto, para evitar que seja demasiado oneroso, o responsável pelo tratamento pode apresentar uma notificação «agregada», que represente todas estas violações, desde que digam respeito ao mesmo tipo de dados pessoais violados da mesma maneira, num espaço de tempo relativamente curto. Se ocorrerem várias violações que digam respeito a diferentes tipos de dados pessoais, violados de maneiras diferentes, então, a notificação deve prosseguir de forma normal, com cada violação a ser comunicada de acordo com o artigo 33.º.

Embora o RGPD permita, até certo ponto, notificações atrasadas, tal não deve ser visto como algo que acontece frequentemente. Vale a pena salientar que as notificações agregadas também podem ser efetuadas para violações múltiplas semelhantes comunicadas no prazo de 72 horas.

C. Violações transfronteiriças e violações em estabelecimentos exteriores à UE

1. Violações transfronteiriças

Quando existe um tratamento transfronteiriço[19] de dados pessoais, uma violação pode afetar titulares de dados em mais de um Estado-Membro. O artigo 33.º, n.º 1, esclarece que quando ocorre uma violação, o responsável pelo tratamento deve notificar a autoridade de controlo competente de acordo com o artigo 55.º do RGPD20. O artigo 55.º, n.º 1, determina o seguinte:

«As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro.»

No entanto, o artigo 56.º, n.º 1, prevê o seguinte:

«Sem prejuízo do disposto no artigo 55.º, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante nos termos do artigo 60.º.»

---

[19] Ver artigo 4.º, n.º 23.

[20] Ver igualmente o considerando 122.

O artigo 56.º, n.º 6, acrescenta:

«A autoridade de controlo principal é o único interlocutor do responsável pelo tratamento ou do subcontratante no tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante.»

Isto significa que, sempre que ocorra uma violação no contexto do tratamento transfronteiriço e seja exigida notificação, o responsável pelo tratamento necessitará de notificar a autoridade de controlo principal[21]. Por conseguinte, ao elaborar o seu plano de resposta a violações, um responsável pelo tratamento deve determinar qual a autoridade de controlo que corresponde à autoridade de controlo principal que deverá notificar[22]. Tal permitirá ao responsável pelo tratamento responder rapidamente a uma violação e cumprir as suas obrigações no que respeita ao artigo 33.º. Deve ficar claro que no caso de uma violação que envolva o tratamento transfronteiriço, a notificação deve ser feita à autoridade de controlo principal, que não se encontra necessariamente onde os titulares de dados afetados estão localizados, ou mesmo onde a violação ocorreu. Ao notificar a autoridade principal, o responsável pelo tratamento deve indicar, se necessário, se a violação envolve estabelecimentos localizados noutros Estados-Membros e em que Estados-Membros é provável que os titulares de dados tenham sido afetados pela violação. Se o responsável pelo tratamento tiver alguma dúvida quanto à identidade da autoridade de controlo principal deve, pelo menos, notificar a autoridade de controlo local onde a violação ocorreu.

[21] Ver orientações do GT29 para a identificação da autoridade de controlo principal de um responsável pelo tratamento ou subcontratante, disponível em http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[22] Pode encontrar-se uma lista de dados de contacto de todas as autoridades nacionais de proteção de dados europeias em: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

2. Violações em estabelecimentos exteriores à UE

O artigo 3.º diz respeito ao âmbito de aplicação territorial do RGPD, inclusive quando é aplicável ao tratamento de dados pessoais efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na UE. Em especial, o artigo 3.º, n.º 2, especifica23 o seguinte:

«O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; ou
b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.»

O artigo 3.º, n.º 3, também é relevante e refere o seguinte24:

«O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado Membro por força do direito internacional público.»

Se um responsável pelo tratamento não estabelecido na UE estiver sujeito ao artigo 3.º, n.º 2, ou ao artigo 3.º, n.º 3, e tiver sido alvo de uma violação, continua vinculado pelas obrigações de notificação nos termos dos artigos 33.º e 34.º. O artigo 27.º exige que um responsável pelo tratamento (e subcontratante) designe um representante na UE onde for aplicável o artigo 3.º, n.º 2. Nestes casos, o GT29 recomenda que a notificação seja feita à autoridade de controlo no Estado-Membro onde o representante do responsável pelo tratamento na UE está estabelecido[25]. De igual modo, se um subcontratante estiver sujeito ao artigo 3.º, n.º 2, ficará vinculado pelas obrigações que incumbem aos subcontratantes, de especial pertinência aqui, o dever de notificar o responsável pelo tratamento de acordo com o artigo 33.º, n.º 2.

---

[23] Ver também os considerandos 23 e 24.

[24] Ver igualmente o considerando 25.

[25] Ver o considerando 80 e o artigo 27.º.

D. Condições em que não é exigida notificação

O artigo 33.º, n.º 1, esclarece que as violações que «não sejam suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares» não exigem notificação à autoridade de controlo. Um exemplo disto pode ser quando os dados pessoais já se encontram disponíveis ao público e uma divulgação desses dados não constitui um risco provável para a pessoa. Isto contraria os requisitos de notificação de violações para os fornecedores de serviços de comunicações eletrónicas acessíveis ao público existentes na Diretiva 2009/136/CE, que prevê que todas as violações relevantes devem ser notificadas à autoridade competente.

No seu Parecer 03/2014 relativo à notificação de violação[26], o GT29 explicou que uma violação da confidencialidade de dados pessoais que tenham sido encriptados com um algoritmo de ponta constitui, ainda assim, uma violação de dados pessoais, e deve ser notificada. No entanto, se a confidencialidade da chave estiver intacta – ou seja, a chave não foi comprometida numa qualquer violação da segurança e tiver sido gerada de modo que não possa ser determinada através de meios eletrónicos disponíveis por qualquer pessoa que não esteja autorizada a aceder-lhe – então, os dados são, em princípio, ininteligíveis. Logo, é pouco provável que a violação afete negativamente as pessoas em causa e, por conseguinte, não exige a comunicação a essas pessoas[27]. No entanto, mesmo quando os dados se encontram encriptados, uma perda ou alteração podem ter consequências negativas para os titulares de dados quando o responsável pelo tratamento não possui cópias de segurança adequadas. Neste caso, a comunicação aos titulares de dados seria exigida, mesmo que os próprios dados tivessem sido sujeitos a medidas de encriptação adequadas.

O GT29 explicou igualmente que este também seria o caso se os dados pessoais, como palavras-passe, foram colocados em *hash* de forma segura e salgados (*salted*), o valor *hash* foi calculado com uma função *hash* de ponta encriptada com chave, a chave utilizada para codificar os dados não foi posta em causa em qualquer violação da segurança, e essa mesma chave foi gerada de modo a que não possa ser determinada, através de meios eletrónicos disponíveis, por qualquer pessoa que não esteja autorizada a aceder a ela.

---

[26] GT29, Parecer 03/2014 relativo à notificação de violação, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[27] Ver também o artigo 4.º, n.os 1 e 2, do Regulamento (UE) n.º 611/2013.

Consequentemente, se os dados pessoais foram tornados essencialmente ininteligíveis para partes não autorizadas e sempre que os dados forem uma cópia ou exista uma cópia de segurança, uma violação da confidencialidade que envolva dados pessoais encriptados pode não precisar de ser notificada à autoridade de controlo. Isto porque tal violação não é suscetível de pôr em risco os direitos e liberdades das pessoas singulares. Tal significa, obviamente, que a pessoa também não necessitaria de ser informada, uma vez que provavelmente não existe risco elevado. No entanto, há que ter presente que, embora a notificação possa não ser exigida inicialmente, se não existir risco provável para os direitos e liberdades das pessoas, isto pode mudar com o decorrer do tempo e o risco teria de ser reavaliado. Por exemplo, se a chave for posteriormente considerada comprometida, ou for exposta uma vulnerabilidade no *software* de encriptação, então, a notificação pode ser exigida.

Além disso, deve observar-se que, se existir uma violação quando não existem cópias de segurança dos dados pessoais encriptados, então, terá ocorrido uma violação da disponibilidade, que pode colocar riscos para as pessoas e, por conseguinte, exigir notificação. De igual modo, sempre que ocorre uma violação que envolve a perda de dados encriptados, mesmo que exista uma cópia de segurança dos dados pessoais, esta pode ser uma violação comunicável, dependendo do tempo que se demora a restaurar os dados a partir dessa cópia de segurança e o efeito que a falta de disponibilidade tem para as pessoas. Como estabelecido no artigo 32.º, n.º 1, um importante fator de segurança é «a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico».

Por exemplo, uma violação que não exigiria notificação à autoridade de controlo seria a perda de um dispositivo móvel encriptado de forma segura, utilizado pelo responsável pelo tratamento e pelo seu pessoal. Desde que a chave de encriptação permaneça em segurança na posse do responsável pelo tratamento e que esta não seja a única cópia dos dados pessoais, então, os dados pessoais não estariam acessíveis a um atacante. Isto significa que a violação não é suscetível de resultar num risco para os direitos e liberdades dos titulares de dados em causa. Se, mais tarde, se tornar evidente que a chave de encriptação foi comprometida ou que o software ou algoritmo de encriptação é vulnerável, o risco para os direitos e liberdades das pessoas singulares muda e, assim, a notificação pode ser exigida.

No entanto, existirá um incumprimento do artigo 33.º sempre que um responsável pelo tratamento não notificar a autoridade de controlo numa situação em que os dados não tenham sido verdadeiramente encriptados de forma segura. Por conseguinte, quando escolhem o *software* de encriptação, os

responsáveis pelo tratamento devem avaliar cuidadosamente a qualidade e a aplicação adequada da encriptação oferecida, compreender qual o nível de proteção que este realmente proporciona e se é adequado aos riscos apresentados. Os responsáveis pelo tratamento devem também estar familiarizados com as especificidades de como o seu produto de encriptação funciona.

Por exemplo, um dispositivo pode ser encriptado assim que é desligado, mas não enquanto está em modo de espera. Alguns produtos que utilizam a encriptação têm «chaves predefinidas» que devem ser alteradas por cada cliente para que sejam eficazes. A encriptação também pode ser considerada atualmente adequada por peritos em segurança, mas pode ficar desatualizada em poucos anos, o que significa que é questionável se os dados seriam suficientemente encriptados por esse produto e se este fornece um nível adequado de proteção.

III. **Artigo 34.º – Comunicação ao titular dos dados**

A. Informar as pessoas singulares

Nalguns casos, para além de notificar a autoridade de controlo, também é exigido que o responsável pelo tratamento comunique uma violação às pessoas afetadas.

O artigo 34.º, n.º 1, estabelece o seguinte:

«Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.»

Os responsáveis pelo tratamento devem recordar-se de que a notificação à autoridade de controlo é obrigatória, a menos que não seja suscetível a existência de um risco para os direitos e liberdades das pessoas em resultado de uma violação. Além disso, quando for suscetível a existência de um risco elevado para os direitos e liberdades das pessoas em resultado de uma violação, as pessoas também devem ser informadas. O limite para a comunicação de uma violação às pessoas é, por conseguinte, mais elevado do que para a notificação das autoridades de controlo e, portanto, nem todas as violações terão de ser comunicadas às pessoas, protegendo-as assim da desnecessária fadiga da notificação.

O RGPD estabelece que a comunicação de uma violação às pessoas singulares deve ser efetuada «sem demora injustificada», o que significa o mais rapidamente possível. O objetivo principal da notificação às pessoas singulares consiste na prestação de informações específicas acerca das medidas que devem tomar para se protegerem[28]. Como observado acima, dependendo da natureza da violação e do risco que coloca, a comunicação atempada irá ajudar as pessoas a tomarem medidas para se protegerem de quaisquer consequências negativas de uma violação.

O anexo B das presentes orientações fornece uma lista não exaustiva de exemplos de quando uma violação é suscetível de resultar num risco elevado para as pessoas e, consequentemente, as circunstâncias em que um responsável pelo tratamento terá que notificar uma violação aos afetados.

B. Informações a comunicar

No que toca a notificar as pessoas, o artigo 34.º, n.º 2, especifica o seguinte:

«A comunicação ao titular dos dados a que se refere o n.º 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 33.º, n.º 3, alíneas b), c) e d).»

De acordo com esta disposição, o responsável pelo tratamento deve, pelo menos, prestar as seguintes informações:

- uma descrição da natureza da violação;
- o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto;
- uma descrição das consequências prováveis da violação; e
- uma descrição das medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Como exemplo das medidas tomadas para reparar a violação e atenuar os seus eventuais efeitos adversos, o responsável pelo tratamento poderia declarar que, após ter notificado a violação à autoridade de controlo relevante, recebeu aconselhamento sobre como gerir a violação e diminuir o seu impacto. O responsável pelo tratamento deve também, se necessário, prestar aconselhamento específico às pessoas para que estas se protejam de possíveis consequências adversas da violação,

[28] Ver igualmente o considerando 86.

como a redefinição de palavras-passe no caso das suas credenciais de acesso terem sido comprometidas. Uma vez mais, o responsável pelo tratamento pode optar por fornecer informação para além da que aqui é exigida.

C. Contactar as pessoas singulares

Em princípio, a violação relevante deve ser comunicada diretamente aos titulares de dados afetados, a menos que isso implique um esforço desproporcionado. Nesse caso, deve ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados sejam informados de forma igualmente eficaz [artigo 34.º, n.º 3, alínea c)].

Devem ser utilizadas mensagens específicas ao comunicar uma violação aos titulares de dados e não devem ser enviadas com outras informações, tais como atualizações regulares, boletins informativos ou mensagens normalizadas. Isto ajuda a tornar a comunicação de uma violação clara e transparente.

Os exemplos de métodos de comunicação transparente incluem o envio direto de mensagens (por exemplo, correio eletrónico, SMS, mensagem direta), faixas ou notificação de sítios Web proeminentes, comunicações postais e anúncios em destaque nos meios de comunicação impressos. Uma notificação confinada apenas a um comunicado de imprensa ou blogue empresarial não seria um meio eficaz para comunicar uma violação a uma pessoa singular. O GT29 recomenda que os responsáveis pelo tratamento escolham um meio que maximize a possibilidade de comunicar informações de forma adequada a todas as pessoas afetadas. Dependendo das circunstâncias, isto pode implicar que o responsável pelo tratamento utilize vários métodos de comunicação, ao invés de utilizar um único canal de contacto.

Os responsáveis pelo tratamento também podem necessitar de garantir que a comunicação esteja acessível em formatos alternativos apropriados e línguas relevantes, por forma a assegurar que as pessoas são capazes de compreender a informação que lhes está a ser prestada. Por exemplo, ao comunicar uma violação a uma pessoa, a língua utilizada durante o curso normal da atividade anterior com o destinatário será, geralmente, apropriada. No entanto, se a violação afetar titulares de dados com quem o responsável pelo tratamento não interagiu previamente, ou em especial aqueles que residem num Estado-Membro ou num país terceiro diferente daquele onde o responsável pelo tratamento se encontra estabelecido, a comunicação na língua nacional local pode ser aceitável, tendo em conta o recurso exigido. O que é importante é ajudar os titulares de dados a compreender a natureza da violação e as medidas que podem tomar para se protegerem.

Os responsáveis pelo tratamento são quem está em melhor posição para determinar o canal de contacto mais adequado para comunicar a violação às pessoas, sobretudo se interagem com os seus clientes frequentemente. No entanto, é evidente que o responsável pelo tratamento deve ter cuidado ao utilizar um canal de contacto comprometido pela violação, pois esse canal também pode ser utilizado por atacantes a fazerem-se passar pelo responsável pelo controlo.

Simultaneamente, o considerando 86 explica o seguinte:

«Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação.»

Por conseguinte, os responsáveis pelo tratamento podem desejar contactar e consultar a autoridade de controlo, não apenas para obterem aconselhamento sobre como informar os titulares de dados de uma violação em conformidade com o artigo 34.º, mas também sobre as mensagens apropriadas a enviar e a maneira mais apropriada para contactar as pessoas singulares.

O considerando 88 contém uma orientação relacionada com o que precede, ou seja, que a notificação de uma violação deve «ter em conta os legítimos interesses das autoridades de polícia nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais». Isso pode significar que, em determinadas circunstâncias, sempre que se justifique e mediante o aconselhamento das autoridades de polícia, o responsável pelo tratamento pode atrasar a comunicação da violação às pessoas afetadas até que isso não prejudique essas investigações. No entanto, os titulares de dados ainda precisariam de ser informados imediatamente após esse período.

Sempre que não seja possível ao responsável pelo tratamento comunicar uma violação a uma pessoa singular devido à insuficiência de dados armazenados para contactar a mesma, nessa circunstância específica, o responsável pelo tratamento deve informar a pessoa logo que razoavelmente possível (por exemplo, quando uma pessoa exerce o seu direito previsto no artigo 15.º de aceder aos dados pessoais e fornece ao responsável pelo tratamento informação suplementar para a contactarem).

D. Condições em que não é exigida comunicação

O artigo 34.º, n.º 3, prevê três condições que, se preenchidas, não exigem notificação às pessoas singulares em caso de violação. A saber:

- O responsável pelo tratamento tiver aplicado medidas técnicas e organizativas adequadas para proteger os dados pessoais antes da violação, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder-lhes. Tal pode incluir, por exemplo, a proteção de dados pessoais com encriptação de ponta, ou através de codificação.
- Imediatamente a seguir a uma violação, o responsável pelo tratamento tiver tomado medidas para assegurar que o risco elevado colocado aos direitos e liberdades das pessoas singulares já

  não é suscetível de se concretizar. Por exemplo, dependendo das circunstâncias do caso, o responsável pelo tratamento pode ter identificado imediatamente e tomado medidas contra a pessoa que acedeu aos dados pessoais antes de esta ter conseguido fazer alguma coisa com eles. Ainda devem ser tidas em devida consideração as possíveis consequências de qualquer violação da confidencialidade, dependendo, mais uma vez, da natureza dos dados em causa.
- Contactar as pessoas singulares implicar um esforço desproporcionado[29], talvez quando os seus dados de contacto se tiverem perdido em resultado da violação ou nunca tiverem sido conhecidos. Por exemplo, o armazém de um gabinete de estatística ficou inundado e os documentos que continham dados pessoais encontravam-se armazenados apenas em papel. Nesse caso, o responsável pelo tratamento deve fazer uma comunicação pública ou tomar uma medida semelhante através da qual as pessoas singulares são informadas de forma igualmente eficaz. No caso de um esforço desproporcionado, também poderiam ser previstas disposições técnicas para disponibilizar a informação sobre a violação a pedido, o que poderia ser útil para aquelas pessoas que podem ser afetadas por uma violação, mas que o responsável pelo controlo não consegue contactar.

[29] Ver orientações do GT29 sobre a transparência, que têm em conta a questão do esforço desproporcionado, disponíveis em http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

De acordo com o princípio da responsabilidade, os responsáveis pelo tratamento devem poder comprovar à autoridade de controlo que preenchem uma ou mais destas condições[30]. Há que ter presente que, embora a notificação possa não ser exigida inicialmente, se não existir risco provável para os direitos e liberdades das pessoas singulares, isto pode mudar com o decorrer do tempo e o risco teria de ser reavaliado.

Se um responsável pelo tratamento decidir não comunicar uma violação à pessoa singular, o artigo 34.º, n.º 4, explica que a autoridade de controlo pode exigir-lhe que o faça, se considerar que a violação é suscetível de resultar num risco elevado para as pessoas singulares. Por outro lado, pode considerar que as condições previstas no artigo 34.º, n.º 3, se encontram preenchidas e, nesse caso, não é exigida a notificação às pessoas singulares. Se a autoridade de controlo determinar que a decisão de não notificar os titulares dos dados não se encontra bem fundamentada, pode considerar a possibilidade de utilizar os seus poderes e sanções disponíveis.

IV. **Avaliar o risco e o risco elevado**

A. O risco como um estímulo para a notificação

Apesar do RGPD introduzir a obrigação de notificar uma violação, não é obrigatório fazê-lo em todas as circunstâncias.

- A notificação à autoridade de controlo é obrigatória, a menos que uma violação não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.
- A comunicação de uma violação às pessoas singulares só é acionada quando é suscetível de resultar num risco elevado para os seus direitos e liberdades.

Isto significa que, logo após ter tido conhecimento de uma violação, é muito importante que o responsável pelo tratamento procure não só conter o incidente, mas também avaliar o risco que dele pode resultar. Existem duas razões importantes para isso: em primeiro lugar, conhecer a probabilidade e a potencial gravidade do impacto sobre as pessoas irá ajudar o responsável pelo tratamento a tomar medidas eficazes para conter e dar resposta à violação; em segundo lugar, irá ajudar a determinar se é exigida notificação à autoridade de controlo e, se necessário, às pessoas em causa.

[30] Ver o artigo 5.º, n.º 2.

Conforme explicado acima, a notificação de uma violação é exigida, a menos que não seja suscetível de resultar num risco para os direitos e liberdades das pessoas, e o estímulo principal que exige a comunicação de uma violação aos titulares de dados é esta ser suscetível de resultar num risco *elevado* para os direitos e liberdades das pessoas. Este risco existe quando a violação pode causar danos físicos, materiais ou imateriais às pessoas cujos dados foram violados. Exemplos deste danos são a discriminação, o roubo ou a usurpação de identidade, as perdas financeiras e os danos para a reputação. Quando a violação envolver dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas, tais danos devem ser considerados suscetíveis de ocorrer[31].

B. Fatores a ter em conta ao avaliar o risco

Os considerandos 75 e 76 do RGPD sugerem que, de um modo geral, ao avaliar o risco, devem ser tidas em conta a probabilidade e a gravidade do risco para os direitos e liberdades dos titulares de dados. Declaram ainda que o risco deve ser aferido com base numa avaliação objetiva.

Deve salientar-se que a avaliação do risco para os direitos e liberdades das pessoas em resultado de uma violação tem uma incidência diferente do que para o risco considerado numa AIPD[32]. A AIPD tem em conta tanto os riscos do tratamento de dados a ser realizado conforme planeado como os riscos em caso de violação. Ao considerar uma potencial violação, analisa em termos gerais a probabilidade da sua ocorrência e os danos que dela podem resultar para os titulares de dados; dito de outra maneira, consiste na avaliação de um evento hipotético. Com uma violação real, o evento já ocorreu e, como tal, incide inteiramente sobre o risco resultante do impacto da violação sobre as pessoas.

Se uma AIPD sugere, por exemplo, que a proposta de utilização de um produto de software de segurança específico para proteger os dados pessoais é uma medida adequada para assegurar um nível de segurança adequado ao risco que, de outra forma, o tratamento podia apresentar para as pessoas. No entanto, se uma vulnerabilidade se tornar posteriormente conhecida, isso alteraria a adequação do software para conter o risco para os dados pessoais protegidos e, como tal, necessitaria de ser reavaliado como parte de uma AIPD em curso.

---

[31] Ver considerandos 75 e 85.

[32] Ver as orientações do GT29 sobre as AIPD aqui: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Uma vulnerabilidade no produto é posteriormente explorada e ocorre uma violação. O responsável pelo tratamento deve avaliar as circunstâncias específicas da violação, os dados afetados, o nível potencial de impacto sobre as pessoas, bem como a probabilidade de o risco se concretizar.

Por conseguinte, ao avaliar o risco para as pessoas em resultado de uma violação, o responsável pelo tratamento deve ter em conta as circunstâncias específicas da violação, incluindo a gravidade do impacto potencial e a probabilidade de que este ocorra. O GT29 recomenda que a avaliação tenha em conta os seguintes critérios[33]: Tipo de violação

O tipo de violação que ocorreu pode afetar o nível de risco para as pessoas. Por exemplo, uma violação da confidencialidade em que foi divulgada informação médica a partes não autorizadas pode ter um conjunto de consequências diferente para uma pessoa do que uma violação em que os dados médicos dessa pessoa se perderam e já não se encontram disponíveis.

- Natureza, sensibilidade e volume dos dados pessoais

Claro que, ao avaliar o risco, um fator importante é o tipo e a sensibilidade dos dados pessoais que foram afetados pela violação. Normalmente, quanto mais sensível forem os dados mais elevado será o risco de dano para a pessoa afetada, mas deve também ser dada atenção a outros dados pessoais que podem já estar disponíveis sobre o titular de dados. Por exemplo, a divulgação do nome e morada de uma pessoa em circunstâncias normais não é suscetível de causar dano substancial. No entanto, se o nome e a morada de um pai adotivo forem divulgados ao pai biológico, as consequências podem ser muito graves para o pai adotivo e para a criança.

As violações que envolvem dados relativos à saúde, documentos de identificação, ou dados financeiros como dados do cartão de crédito, podem todas causar dano por si mesmas, mas se utilizadas em conjunto podem ser utilizadas para roubo de identidade. A combinação de dados pessoais é tipicamente mais sensível do que um único dado pessoal.

[33] O artigo 3.º, n.º 2, do Regulamento (UE) n.º 611/2013 fornece orientações sobre os fatores que devem ser tidos em consideração em relação à notificação de violações no setor dos serviços de comunicações eletrónicas, que podem ser úteis no contexto da notificação ao abrigo do RGPD. Ver https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:pt:PDF.

Alguns tipos de dados pessoais podem parecer à primeira vista relativamente inócuos; contudo, o que esses dados podem revelar sobre a pessoa afetada deve ser cuidadosamente considerado. Uma lista de clientes que aceitam entregas regulares pode não ser especialmente sensível, mas os mesmos dados sobre clientes que solicitaram que as suas entregas fossem interrompidas durante as férias seriam informações úteis para os criminosos.

Do mesmo modo, uma pequena quantidade de dados pessoais altamente sensíveis pode ter um impacto elevado numa pessoa, e uma grande variedade de dados pode revelar um maior leque de informações sobre essa pessoa. Além disso, uma violação que afeta grandes volumes de dados pessoais sobre muitos titulares de dados pode ter um efeito sobre um grande número correspondente de pessoas.

- Facilidade de identificação de pessoas singulares

Um fator importante a ter em conta é quão fácil será para um terceiro que tenha acesso a dados pessoais afetados identificar pessoas específicas ou combinar os dados com outras informações para identificar pessoas. Dependendo das circunstâncias, a identificação poderia ser possível diretamente a partir dos dados pessoais violados sem ser necessária nenhuma pesquisa especial para descobrir a identidade da pessoa, ou pode ser extremamente difícil fazer corresponder dados pessoais a uma pessoa específica, mas continuar a ser possível sob certas condições. A identificação pode ser direta ou indiretamente possível a partir dos dados violados, mas pode depender também do contexto específico da violação e da disponibilidade ao público dos dados pessoais revelados. Isto pode ser mais pertinente para as violações da confidencialidade e da disponibilidade.

Conforme indicado acima, os dados pessoais protegidos por um nível de encriptação adequado serão ininteligíveis para pessoas não autorizadas sem uma chave de decifração. Além disso, uma pseudonimização aplicada de forma adequada (definida no artigo 4.º, n.º 5, como «o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável») também pode reduzir a probabilidade de as pessoas serem identificadas no caso de uma violação. No entanto, as técnicas de pseudonimização, por si mesmas, não podem ser consideradas como tornando os dados ininteligíveis.

Gravidade das consequências para as pessoas.

Dependendo da natureza dos dados pessoais envolvidos numa violação, por exemplo, das categorias especiais de dados, o dano potencial para as pessoas decorrente pode ser especialmente severo, em especial se a violação resultar em roubo ou usurpação de identidade, dano físico, distúrbios psicológicos, humilhação ou dano para a reputação. Se a violação disser respeito a dados pessoais de pessoas vulneráveis, estas podem ser colocadas em maior risco de dano.

Se o responsável pelo tratamento está ciente, ou não, de que os dados pessoais estão nas mãos de pessoas cujas intenções são desconhecidas ou possivelmente maliciosas, pode influenciar o nível de risco potencial. Pode ocorrer uma violação da confidencialidade, em que os dados pessoais são divulgados por engano a um terceiro, conforme definido no artigo 4.º, n.º 10, ou a outro destinatário. Isto pode acontecer, por exemplo, quando os dados pessoais são enviados acidentalmente para o departamento errado de uma organização, ou para uma organização fornecedora comumente utilizada. O responsável pelo tratamento pode solicitar que o destinatário devolva ou destrua de forma segura os dados que recebeu. Em ambos os casos, dado que o responsável pelo tratamento tem um relação contínua com eles, e pode ter conhecimento dos seus procedimentos, história e outros pormenores relevantes, o destinatário pode ser considerado «de confiança». Dito de outra maneira, o responsável pelo tratamento pode ter um nível de confiança com o destinatário para que possa razoavelmente esperar que a parte não leia ou aceda aos dados enviados por engano e cumpra as suas instruções para os devolver. Mesmo que os dados tenham sido acedidos, o responsável pelo tratamento poderia ainda confiar que o destinatário não tomasse mais nenhuma medida e os devolvesse rapidamente e cooperasse na sua recuperação. Nesses casos, isto pode ser tido em conta na avaliação do risco efetuada pelo responsável pelo tratamento na sequência de uma violação – o facto de o destinatário ser confiável pode erradicar a gravidade das consequências da violação, mas não significa que esta não ocorreu. No entanto, isso pode, por sua vez, eliminar a probabilidade de risco para as pessoas, deixando de ser exigida notificação à autoridade de controlo ou às pessoas afetadas. Mais uma vez, isso dependerá de cada caso. Contudo, o responsável pelo tratamento ainda tem de guardar as informações referentes à violação como parte do dever geral de conservar registos de violações (ver secção V abaixo).

Deve ter-se em conta a permanência das consequências para as pessoas, em que o impacto pode ser considerado maior se os efeitos foram de longo prazo.

- Características especiais das pessoas singulares

Uma violação pode afetar os dados pessoais relativos a crianças ou outras pessoas vulneráveis, que podem ser postas em grande risco de perigo em resultado dela. Podem existir outros elementos sobre a pessoa que podem afetar o nível do impacto da violação sobre ela.

- Características especiais do responsável pelo tratamento de dados

A natureza e o papel do responsável pelo tratamento e das suas atividades podem afetar o nível de risco para as pessoas resultante de uma violação. Por exemplo, uma organização médica irá tratar categorias especiais de dados pessoais, o que significa que existe uma ameaça maior para as pessoas, se os seus dados pessoais forem violados, em comparação com a lista de distribuição de um jornal.

- Número de pessoas afetadas

Uma violação pode afetar apenas uma ou poucas pessoas ou várias centenas, se não mais. De um modo geral, quanto maior for o número de pessoas afetadas maior é o impacto que uma violação pode ter. No entanto, uma violação pode ter um impacto grave numa só pessoa, dependendo da natureza dos dados pessoais e do contexto em que foram afetados. Mais uma vez, o fundamental é ter em conta a probabilidade e a gravidade do impacto sobre as pessoas afetadas.

Elementos gerais

Por conseguinte, ao avaliar o risco suscetível de resultar de uma violação, o responsável pelo tratamento deve ter em conta uma combinação da gravidade do impacto potencial sobre os direitos e liberdades das pessoas e da probabilidade de este ocorrer. Claramente, se as consequências de uma violação forem mais graves, o risco é mais elevado, se a probabilidade de aquelas ocorrerem for maior, o risco também aumenta. Em caso de dúvida, o responsável pelo tratamento deve optar pela precaução e notificar. O anexo B fornece alguns exemplos úteis de diferentes tipos de violações que envolvem risco ou risco elevado para as pessoas.

A Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) elaborou recomendações para uma metodologia de avaliação da gravidade de uma violação, que os

responsáveis pelo tratamento e subcontratantes podem considerar útil na elaboração do seu plano de resposta para a gestão de violações[34].

V. Responsabilidade e manutenção de registos

A. Documentação de violações

Independentemente de uma violação necessitar ou não de ser notificada à autoridade de controlo, o responsável pelo tratamento deve conservar a documentação de todas as violações, como o artigo 33.º, n.º 5, explica o seguinte:

«O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.»

Isto está relacionado com o princípio da responsabilidade do RGPD, constante do artigo 5.º, n.º 2. O objetivo de registar violações não notificáveis, assim como violações notificáveis, também está relacionado com as obrigações do responsável pelo tratamento previstas no artigo 24.º e a autoridade de controlo pode exigir ver estes registos. Os responsáveis pelo tratamento são, por conseguinte, encorajados a criar um registo interno de violações, independentemente de terem de notificar ou não[35].

Embora caiba ao responsável pelo tratamento determinar que método e estrutura utilizar na documentação de uma violação, em termos de informação registada, existem elementos-chave que devem ser incluídos em todos os casos. Como exigido pelo artigo 33.º, n.º 5, o responsável pelo tratamento deve registar as informações relativas à violação, que devem incluir as suas causas, o que aconteceu e os dados pessoais afetados. Deve também incluir os efeitos e consequências da violação, juntamente com a medida de reparação adotada pelo responsável pelo tratamento. O RGPD não especifica o período de conservação dessa documentação. Quando esses registos contiverem dados

[34] ENISA, Recomendações para uma metodologia de avaliação da gravidade das violações de dados pessoais, https://www.enisa.europa.eu/publications/dbn-severity

[35] O responsável pelo tratamento pode optar por documentar as violações como parte do seu registo de atividades de tratamento mantido de acordo com o artigo 30.º. Não é necessário um registo separado, desde que a informação relevante para a violação seja claramente identificável como tal e possa ser extraída mediante pedido.

pessoais, caberá ao responsável pelo tratamento determinar o período apropriado de conservação em conformidade com os princípios relacionados com o tratamento de dados pessoais[36] e atender a uma base legal para o tratamento[37]. Será necessário conservar a documentação de acordo com o artigo 33.º, n.º 5, na medida em que pode ser chamado a fornecer prova do cumprimento do disposto nesse artigo ou, de um modo mais geral, com o princípio da responsabilidade, à autoridade de controlo. É claro que, se os próprios registos não contiverem dados pessoais, então, o princípio da limitação da conservação[38] do RGPD não se aplica.

Além destas informações, o GT29 recomenda que o responsável pelo tratamento também documente a sua fundamentação para as decisões tomadas em resposta a uma violação. Em especial, se uma violação não for notificada, deve ser documentada a justificação para essa decisão. Isto deve incluir as razões pelas quais o responsável pelo tratamento considera que a violação não é suscetível de resultar num risco para os direitos e liberdades das pessoas singulares[39]. Por outro lado, se o responsável pelo tratamento considera que se encontra preenchida qualquer uma das condições que constam do artigo 34.º, n.º 3, então, deve conseguir fornecer prova adequada de que é esse o caso.

Quando o responsável pelo tratamento notifica uma violação à autoridade de controlo, mas a notificação está atrasada, deve ser capaz de justificar esse atraso; a documentação relacionada com isto pode ajudar a demonstrar que o atraso na comunicação é justificado e não excessivo.

Quando o responsável pelo tratamento comunica uma violação às pessoas afetadas, deve ser transparente quanto à violação e comunicar de forma eficaz e atempada. Por conseguinte, a conservação de provas dessa comunicação ajudaria o responsável pelo tratamento a demonstrar responsabilidade e conformidade.

Para ajudar a conformidade com os artigos 33.º e 34.º, seria vantajoso tanto para os responsáveis pelo tratamento como para os subcontratantes adotar um procedimento de notificação documentado, que defina o processo a ser seguido após a deteção de uma violação, incluindo como conter, gerir e recuperar do incidente, bem como avaliar o risco e notificar a violação. A este respeito, por forma a

---

[36] Ver artigo 5.º.

[37] Ver artigo 6.º e também o artigo 9.º.

[38] Ver artigo 5.º, n.º 1, alínea e).

[39] Ver considerando 85.

demonstrar a conformidade com o RGPD, pode também ser útil demonstrar que os trabalhadores foram informados da existência desses procedimentos e mecanismos e que sabem como reagir a violações.

Deve ser observado que a incapacidade de documentar corretamente uma violação pode levar a autoridade de controlo a exercer os seus poderes nos termos do artigo 58.º e/ou a impor uma coima em conformidade com o artigo 83.º.

B. Função do Encarregado da Proteção de Dados

Um responsável pelo tratamento ou um subcontratante pode ter um encarregado da proteção de dados (EPD ou DPO)[40], quer seja exigido pelo artigo 37.º ou de forma voluntária, por uma questão de boas práticas.

O artigo 39.º do RGPD estabelece várias funções obrigatórias para o EPD, mas não impede que sejam atribuídas outras funções pelo responsável pelo tratamento, se necessário.

De especial relevância para a notificação de violações, as funções obrigatórias do EPD incluem, entre outros deveres, prestar aconselhamento e informações sobre proteção de dados ao responsável pelo tratamento e subcontratante, controlar a conformidade com o RGPD e prestar aconselhamento em relação às AIPD. O EPD deve igualmente cooperar com a autoridade de controlo e atuar como ponto de contacto para a autoridade de controlo e para os titulares de dados. Importa notar que, ao notificar a violação à autoridade de controlo, o artigo 33,º, n.º 3, alínea b), exige que o responsável pelo tratamento forneça o nome e os dados de contacto do seu EPD, ou de outro ponto de contacto.

Em termos de documentação de violações, o responsável pelo tratamento ou subcontratante pode desejar obter o parecer do seu EPD quanto à estrutura, elaboração e administração da sua documentação. O EPD pode também ser encarregado de manter esses registos.

Estes elementos significam que o EPD deve desempenhar um papel fundamental na assistência à prevenção ou à preparação para uma violação através da prestação de aconselhamento e do controlo da conformidade, bem como durante uma violação (ou seja, ao notificar a autoridade de controlo), e durante qualquer investigação subsequente por parte da autoridade de controlo. À luz do que precede,

[40] Ver as orientações do GT29 relativas aos EPD aqui: http://ec.europa.eu/newsroom/just/itemdetail.cfm?item_id=50083.

o GT29 recomenda que o EPD seja prontamente informado acerca da existência de uma violação e esteja envolvido em todo o processo de gestão e notificação de violações.

VI. Obrigações de notificação ao abrigo de outros instrumentos jurídicos

Além e à parte da notificação e comunicação de violações ao abrigo do RGPD, os responsáveis pelo tratamento devem também estar cientes de qualquer requisito para notificar incidentes de segurança ao abrigo de outra legislação conexa que lhes possa ser aplicável e se esta também pode exigir que notifiquem a autoridade de controlo de uma violação de dados pessoais ao mesmo tempo. Tais requisitos podem variar entre Estados-Membros, mas os exemplos de requisitos de notificação em outros instrumentos jurídicos e de como estes se interrelacionam com o RGPD incluem o seguinte:

- Regulamento (UE) n.º 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (Regulamento IDeSC)[41].

O artigo 19.º, n.º 2, do Regulamento IDeSC exige que os prestadores de serviços de confiança notifiquem a sua entidade supervisora de uma violação da segurança ou perda de integridade que tenha um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados. Se aplicável – isto é, quando essa violação ou perda é também uma violação de dados pessoais ao abrigo do RGPD – o prestador de serviços de confiança deve também notificar a autoridade de controlo.

- Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI)[42].

Os artigos 14.º e 16.º da Diretiva SRI exigem que os operadores de serviços essenciais e os prestadores de serviços digitais notifiquem incidentes de segurança à sua autoridade competente.

Conforme reconhecido no considerando 63 da SRI[43], os incidentes de segurança podem, muitas vezes, incluir dados pessoais comprometidos. Embora a SRI exija que as autoridades competentes e

---

[41] Ver http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32014R0910

[42] Ver http://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1503582022842&uri=CELEX:32016L1148.

[43] Considerando 63: *«Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção dos dados deverão*

as autoridades de supervisão cooperem e troquem informações nesse contexto, continua a suceder que quando esses incidentes são, ou se tornam, violações de dados pessoais ao abrigo do RGPD, esses operadores e/ou prestadores são obrigados a notificar a autoridade de controlo separadamente dos requisitos de notificação de incidentes da SRI.

Por exemplo, um prestador de serviços de computação em nuvem que notifica uma violação ao abrigo da Diretiva SRI pode também ter de notificar um responsável pelo tratamento, se esta incluir uma violação de dados pessoais. Do mesmo modo, um prestador de serviços de confiança que notifica ao abrigo do IDeSC pode também ser obrigado a notificar a autoridade de proteção de dados relevante no caso de uma violação.

- Diretiva 2009/136/CE (Diretiva Direitos dos Cidadãos) e Regulamento (UE) n.º 611/2013 (Regulamento Notificação de Violações).

Os prestadores de serviços de comunicações eletrónicas disponíveis ao público no contexto da Diretiva 2002/58/CE[44] devem notificar as violações às autoridades nacionais competentes.

Os responsáveis pelo tratamento devem também estar cientes de quaisquer deveres de notificação jurídica, médica ou profissional ao abrigo de outros regimes aplicáveis.

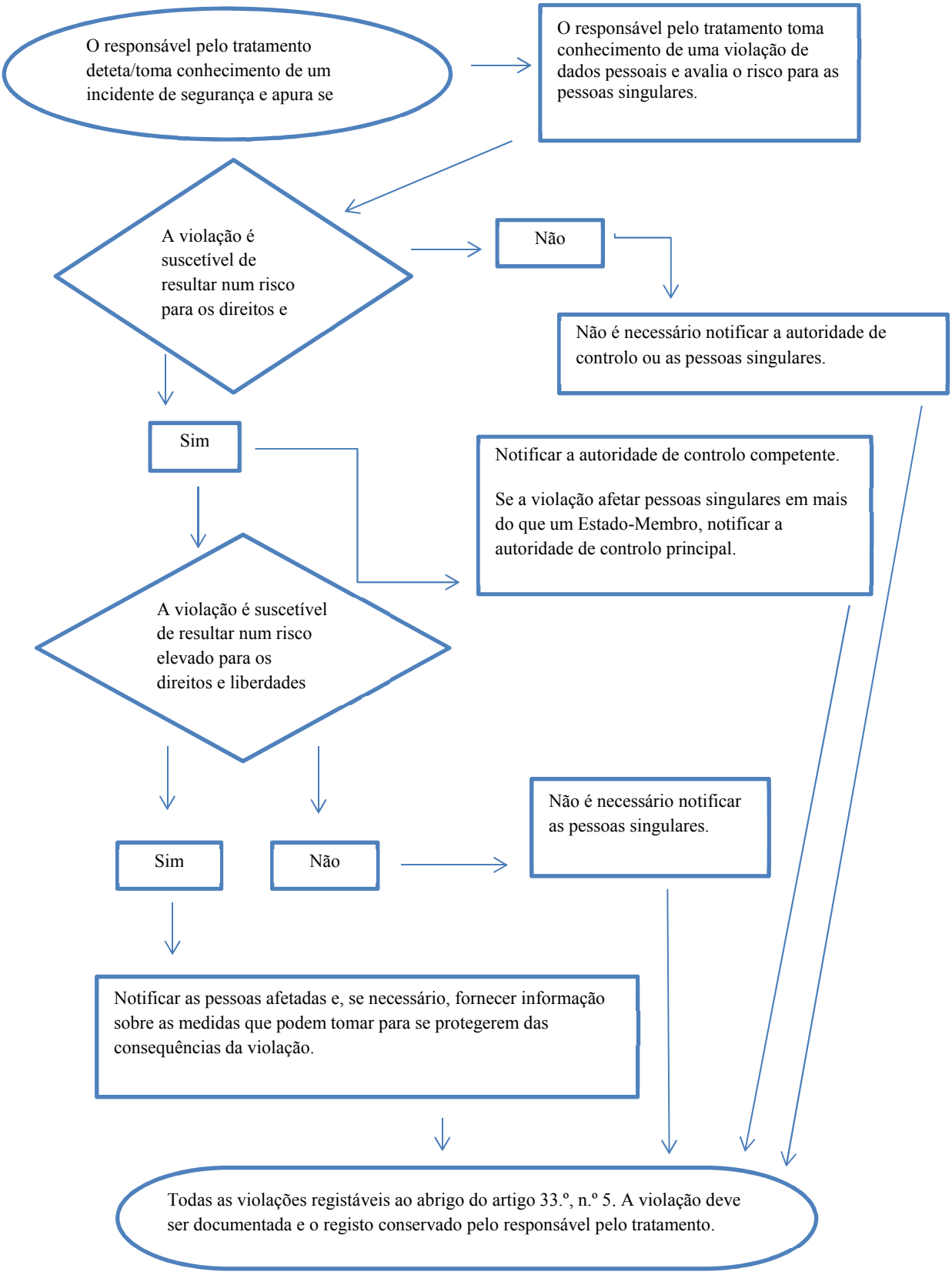
---

cooperar e trocar informações sobre todas as questões pertinentes para combater as eventuais violações de dados pessoais resultantes de incidentes.»

[44] Em 10 de janeiro de 2017, a Comissão Europeia propôs um regulamento relativo à privacidade e às comunicações eletrónicas, que irá substituir a Diretiva 2009/136/CE e remover os requisitos de notificação. No entanto, até que esta proposta seja aprovada pelo Parlamento Europeu, o atual requisito de notificação permanece em vigor, ver https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-andelectronic-communications.

VII. **Anexo**

A. Fluxograma que apresenta os requisitos de notificação



B – Etapas

Passo	Ação recomendada	Comentários
1	**Contactar os departamentos / pessoas relevantes** Esteja preparado para contactar as pessoas chave rapidamente, por exemplo via telefone ou e-mail. Deverá contactar de imediato os seguintes departamentos: • Departamento Jurídico e DPO	O RT deve organizar uma lista de contactos especial para as situações de violação de dados pessoais. Esta lista deve estar sempre atualizada, deve ser divulgada e estar disponível *on-site* (nos computadores da empresa) e *offsite* (em formato pdf e nos contactos dos telemóveis e outros *devices* móveis da entidade).
2	**Iniciar a investigação da eventual violação de dados pessoais e tomar as primeiras medidas de contenção**	
3	**Identificar as obrigações legais** O Departamento Jurídico, em conjunto com o DPO com o auxílio de consultores externos identifica as obrigações legais relevantes, em função dos factos apurados.	Devem ser avaliados os riscos para as pessoas singulares (sem risco, com risco ou com elevado risco) e devem ser informadas as funções / pessoas relevantes da empresa.
4	**Notificar o responsável pelo tratamento (se aplicável)** Nas situações em que esteja a agir na qualidade de subcontratante, deve notificar o responsável pelo tratamento sem demora injustificada após ter conhecimento da violação de dados pessoais.	O RGPD prevê que esta notificação deva ser feita sem demora injustificada. Os responsáveis pelo tratamento podem definir contratualmente prazos concretos a cumprir.
5	**Notificar a CNPD (se aplicável)** A notificação deve ser efetuada sem demora injustificada e, sempre que possível, **até 72 horas após ter tido conhecimento da violação de dados pessoais.** A notificação deve, pelo menos: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou outro ponto de contacto onde possam ser obtidas	A entidade não está obrigada a notificar a CNPD caso a violação de dados pessoais são seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas à CNPD por fases, sem demora injustificada. Se a entidade não tiver já comunicado a violação de dados pessoais ao titular dos dados (nos casos em que esta comunicação é obrigatória), a CNPD pode

	mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	exigir que proceda a essa notificação ou dispensá-la, nos casos previstos no artigo 35.º n.º 3.
6	**Notificar os titulares de dados (se aplicável)** Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica também a violação de dados pessoais ao **titular dos dados**, sem demora injustificada. Esta comunicação deve descrever em linguagem clara e simples a natureza da violação dos dados pessoais e fornecer, pelo menos, as seguintes informações e medidas: a) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; b) Descrever as consequências prováveis da violação de dados pessoais; c) Descrever as medidas adotadas ou propostas pelo responsável de tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	Uma das finalidades da comunicação aos titulares é limitar os danos que estes possam sofrer. A comunicação não é exigida se for preenchida uma das seguintes condições: a) A entidade tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; b) O responsável de tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares já não é suscetível de se concretizar; c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
7	**Documentar a violação de dados pessoais** Este registo deve conter os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada.	Esta documentação deve permitir à CNPD verificar o cumprimento do disposto no art. 33.º do RGPD.
8	**Melhorar os processos internos**	