POLÍTICA DE

RESPOSTAS ÀS VIOLAÇÕES (LGPD)

POLI-0018-01

MANTENHA APENAS UM: CONFIDENCIAL | **RESTRITO** | USO INTERNO | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2021	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0018-01	Política	Restrito

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Respostas à Incidentes (LGPD)
Política de Notificação de Violação de Dados (LGPD)

Aprovação da Diretoria Responsável

Diretor Responsável	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Introdução

A Lei Geral de Proteção de Dados (LGPD) estabelece requisitos de notificação de violação de segurança para controladores e operadores de dados. Este documento explora essas obrigações, levando em conta as lições aprendidas dos requisitos de notificação de violação nos Estados Unidos e Europa.

Conhecendo a LGPD

A Lei Geral de Proteção de dados não tratou de definir o que seria uma violação de dados, contudo, por meio da legislação europeia, pode-se conceituar como sendo:

"*uma violação de 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.*"

Uma vez constatada uma violação e, sendo a violação passível de causar risco ou danos relevantes aos titulares, de acordo com o artigo 48 da LGPD, o controlador deverá, assim que possível, notificar a Autoridade Nacional, bem como o titular dos dados.

Artigo 48: Notificação a Autoridade Nacional e aos Titulares dos Dados acerca de um Risco Decorrente da Violação

> *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares.*
>
> *§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:*

I- A descrição da natureza dos dados pessoais afetados;

II- As informações sobre os titulares envolvidos;

III- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV- Os riscos relacionados ao incidente;

V- Os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I- Ampla divulgação do fato em meios de comunicação; e

II- Medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade de incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados e acessá-los.

Orientações sobre as disposições de notificação de violação de dados pessoais são encontradas no artigo em questão. No mais, havendo a violação de dados e, tendo a Autoridade Nacional detectado que as medidas tomadas pela **Epeople** não sejam eficazes, poderá ainda, por força do artigo 31 da mesma lei *"enviar informe com medidas cabíveis para fazer cessar a violação"*.

Tal como acontece com as leis de notificação de violação dos Estados Unidos e da Europa, as disposições de notificação da LGPD são claramente motivadas pelo desejo de permitir que os titulares de dados minimizem os possíveis danos que possam resultar de uma violação de dados pessoais. No entanto, também está claro que os danos previstos pela LGPD são mais amplos do que os geralmente considerados ao avaliar as violações de dados nos EUA. Como você pode ver

no artigo 48, a violação passível de notificação é aquela que *"possa acarretar risco ou dano relevante aos titulares"*, tais como perda de controle dos seus dados pessoais ou limitação dos seus direitos, discriminação, roubo ou fraude de identidade, perdas financeiras, reversão não autorizada de pseudonimização, danos à reputação, perda de confidencialidade de dados pessoais protegidos pelo segredo profissional ou outras desvantagens económicas ou sociais significativas para a pessoa singular.

A LGPD equilibra essa definição extremamente ampla de danos, definindo um processo de notificação em duas etapas. Se houver algum "risco" ou de "dano", o controlador deve notificar a Autoridade Nacional, bem como o titular dos dados assim que possível.

No mais, a LGPD ainda reflete o consenso regulatório de que a violação deve ser notificada assim que possível, ou seja, de forma rápida. Se o responsável pelo tratamento não puder fornecer essa notificação inicial à Autoridade Nacional e ao titular de dados, deve fornecer uma explicação para o atraso.

O artigo 48 da LGPD prevê que não será necessário a notificação da Autoridade nacional e do titular dos dados se, não houver nenhum risco ou dano relevante aos titulares. Contudo, se o controlador entender que há risco ou dano, ele deve notificar tanto a Autoridade Nacional, quanto os titulares envolvidos de forma mais rápida possível.

A notificação deve ocorrer o mais rapidamente possível, levando em consideração a orientação das autoridades relevantes e outros fatos. "Por exemplo, a necessidade de mitigar um risco imediato de danos exigiria comunicação imediata com os titulares de dados, enquanto a necessidade de implementar medidas apropriadas contra violações de dados pessoais contínuas ou semelhantes pode justificar mais tempo para comunicação.".

O artigo 49 da LGPD ilustra a importância do uso de medidas de segurança apropriadas, *"os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares"*, (como criptografia) para proteger os dados

pessoais. Seguindo a tendência nos EUA e da Europa, a LGPD não fornece uma exceção geral às regras de notificação de violação para dados criptografados. Uma vez ocorrida a violação, sejam os dados criptografados ou não e, sendo passível de risco ou dano, a Autoridade Nacional e o titular de dados têm de ser notificado.

Tal como nos EUA, e na Europa, parece razoável antecipar que a Autoridade Nacional utilizará as notificações de violação como ponto de partida para considerar a adequação das medidas de segurança das organizações inquiridas em geral. Assim, a notificação realizada, também poderá ser vista como ponto de partida para eventuais sanções administrativas.

Assim, é útil entender que a criptografia e tecnologias de proteção de dados também podem fornecer benefícios para programas de respostas a incidentes.

Compliance

Embora as disposições de notificação de violação na LGPD sejam muito específicas em certos aspectos, como o programa de governança e o conteúdo dos avisos, há outras áreas em que as expectativas são indefinidas. Essa incerteza cria riscos para a **Epeople** e, potencialmente, prejudica a eficácia e a oportunidade do processo de notificação. Assim, este documento observa os desafios e oferece algumas opções que podem permitir que o processo de notificação de violação funcione com mais eficiência.

Prazo da Notificação

A LGPD não especifica em dias, ou horas, qual o tempo hábil para realizar a notificação acerca da violação de dados. O Artigo 48, § 1º apenas indica que a notificação deve ser feita em prazo razoável. Por sua vez, a legislação europeia determina que 72 horas é considerado o prazo razoável entre a detecção da violação e a notificação das partes interessadas. Enquanto a Autoridade Nacional não dispor o contrário, entendemos que o prazo para a notificação não deve ultrapassar 72 horas _ até porque, a nossa legislação foi inspirada, quase que na totalidade, na legislação europeia.

Notificação para ANPD

Uma das questões mais difíceis que estão sujeitas a LGPD é determinar quais violações devem ser notificadas para a ANPD. Conforme informado, o artigo 48 da Lei em questão informa que todas as violações passíveis de risco ou dano ao titular dos dados deverá culminar na notificação da Autoridade competente.

Assim como ocorre na legislação Americana, o Brasil exige que havendo uma violação passível de notificação da Autoridade Nacional competente, paralelamente a essa notificação, o titular de dados também deve ser cientificado da violação de seus dados. Nesse modelo, os reguladores tomam conhecimento das violações, para que possam prestar assistência aos indivíduos que os contatam depois de receber uma carta de notificação.

Determinar Riscos e Danos

Se após uma análise a **Epeople** constatar que a violação não causou nenhum/ nem possa causar prejuízo ao titular dos dados, a violação não precisa ser divulgada, contudo, a violação tem de estar registrada nos arquivos da **Epeople**, bem como as medidas utilizadas para sanar a brecha na proteção de dados. Se o risco de um incidente for totalmente mitigado, a **Epeople** não deve notificar os indivíduos.

A notificação excessiva (particularmente quando não há risco de atenuar) pode criar fadiga de notificação e reduzir a probabilidade de que indivíduos atuem em uma carta de notificação, mesmo quando a ação é necessária. Por exemplo, um funcionário da **Epeople** pode inadvertidamente transmitir um arquivo contendo dados pessoais para o destinatário errado. (Um arquivo destinado a um fornecedor da **Epeople** pode ser enviado acidentalmente para outro fornecedor.) Se o destinatário for confiável, o erro é relatado e os dados são recuperados com garantias confiáveis de que não foram armazenados ou usados, não há ou há muito pouco risco para o indivíduo. Esses tipos de incidentes não devem acionar a notificação, pois não há mais riscos a serem gerenciados.

A política segue as melhores práticas do setor de uma abordagem em duas etapas para violações de privacidade:

1º - Os indivíduos correm risco real de sofrer danos? Em caso afirmativo, notifique os indivíduos o quanto antes e forneça assistência para mitigar o risco. Notificar a ANPD e outros (como agências de aplicação da lei, equipes de fraude de cartões de pagamento etc.) conforme apropriado ou necessário.

2º - Se não houver risco de dano e nenhuma obrigação legal de notificar ninguém, documente os resultados e implemente qualquer aprendizado organizacional necessário para reduzir a probabilidade de esse tipo de incidente ocorrer novamente.

Esse modelo pode fornecer à **Epeople** uma base para avaliar e padronizar as expectativas do programa de resposta a incidentes.

Considerações Práticas

A **Epeople** e outras partes interessadas devem colaborar para oferecer respostas às questões práticas que surgirão à medida que a **Epeople** implementa este programa de notificação de violações junto a ANPD. Três desafios específicos envolvem a determinação das melhores formas de reduzir o risco de violações, a comunicação efetiva com o titular de dados sobre violações e a habilitação de operadores de dados para oferecer suporte a controladores em violações grandes de vários clientes.

a) Quais são as formas aceitáveis de mitigação de risco?

Embora seja apropriado entender os riscos que surgem das violações de dados pessoais em geral, devemos reconhecer que nem sempre há maneiras fáceis (ou padronizadas) de mitigar os diferentes tipos de risco. Nos EUA, as leis de notificação de violação se concentram em alertar os indivíduos sobre os riscos de roubo de identidade ou fraude financeira. Esses riscos podem ser mitigados usando serviços que estão amplamente disponíveis nos EUA, como monitoramento de

crédito, serviços de resolução de fraudes e seguro contra roubo de identidade. O sucesso desses produtos é tal que eles geralmente são fornecidos aos indivíduos, mesmo quando uma violação não compromete dados financeiros ou identificadores.

O problema com essa abordagem de "oferecer sempre crédito ao monitoramento", no entanto, é que o remédio muitas vezes não se ajusta ao risco. Se as credenciais da conta online forem comprometidas, o monitoramento de crédito não ajudará. Dessa feita, a melhor forma seria oferecer um programa de proteção on-line, como antivírus ou software de malware, junto com materiais educativos sobre como evitar ataques de *phishing*. Em outras situações, como a divulgação de um fato particular (como salário ou condição médica), pode não haver uma maneira real de mitigar esse dano. Nesse caso, a **Epeople** só pode pedir desculpas e tomar medidas para evitar que esse tipo de violação aconteça novamente.

A lição importante a aprender com os EUA é que empresas, reguladores, ONGs e outros precisam ser flexíveis e criativos ao considerar formas de mitigar os danos. As estratégias de mitigação precisam refletir a situação específica. Seria útil ter uma caixa de ferramentas abrangente de mitigação de riscos com várias ferramentas, como:

- Modelos padrões de contrato para obter garantias de terceiros não autorizados de que eles não usarão ou divulgarão dados pessoais;

- Produtos de monitoramento de crédito (quando disponíveis) e produtos similares de "proteção de identidade" para violações de dados pessoais envolvendo identificadores nacionais, dados de contas financeiras e afins;

- Produtos de proteção on-line, como software antivírus, para violações de dados pessoais que comprometem contas on-line;

- Materiais de educação do consumidor, fornecendo informações específicas que os indivíduos podem usar para lidar com quaisquer danos que tenham. Por exemplo, se uma violação pode colocar um indivíduo em risco de discriminação, a **Epeople** deve educar o titular sobre os

tipos de discriminação que podem ser encontrados e que recurso legal a pessoa pode ter contra a entidade envolvida na conduta ilegal; e

- Educação do titular em relação aos direitos de proteção de dados em geral, e informações sobre como obter assistência com solicitações de acesso, para que o indivíduo possa localizar e solicitar a exclusão de quaisquer dados pessoais que possam ter sido adquiridos por outras pessoas.

b) Como nos Comunicar Efetivamente com o Titular dos Dados?

Nos EUA, as leis de notificação de violação tornaram-se muito específicas no que diz respeito ao conteúdo que deve ser fornecido aos titulares dos dados, incluindo em muitos casos informações sobre relatórios de crédito, relatórios policiais etc. Embora cada um destes tipos de conteúdo possa ser muito útil, conforme mencionado acima, o conteúdo fornecido deve ser adaptado aos tipos específicos de incidentes.

Por exemplo, nos EUA, as cartas de notificação "presumem" que os elementos de dados violados colocam o indivíduo em risco de roubo tradicional de identidade. No entanto, se uma violação comprometer o número do cartão de crédito de um usuário, a pessoa precisará revisar as declarações da conta de cartão de crédito, denunciar cobranças fraudulentas e obter um novo cartão (com um novo número) se o número comprometido estiver sendo usado incorretamente. Um número de cartão de crédito comprometido não cria um risco de que a identidade de uma pessoa seja usada para criar novas contas. Os requisitos legais para o envio da comunicação resultam em indivíduos recebendo notificações com informações que não se encaixam na situação. Essas notificações são confusas e contraproducentes porque não instruem clara e concisa o indivíduo sobre os passos que precisam ser tomados.

Assim como acontece na GDPR europeia, a legislação brasileira, em seu artigo 48, determina que os requisitos de notificação estabelecidos na legislação nos parecem fornecer parâmetros apropriados para a notificação da pessoa em causa. Como parte da construção do conjunto de ferramentas discutido acima, os vários interessados podem desejar desenvolver alguns modelos

padrão para ajudar a assegurar que os titulares de dados obtenham informações apropriadas e eficazes, adaptadas aos riscos apresentados pela violação. O conteúdo da carta de notificação não deve ser um modelo fechado, mas sim adequado para cada tipo de violação.

c) Como os Operadores podem dar Suporte aos Controladores em Violações de Múltiplos clientes?

Por último, é importante considerar também os desafios práticos que existem para as partes interessadas quando ocorre uma grande violação em um processador de dados. Como nos EUA, as regras de notificação de violação antecipam que os operadores notificarão os controladores, para que o controlador possa notificar as Autoriades Competentes e os titulares. No entanto, quando uma violação do operador envolve muitos controladores, o processo de resposta fica atolado. O operador pode estar tentando se comunicar com dezenas ou centenas de seus clientes; esses clientes estarão relatando os fatos em segunda mão para suas autoridades competentes, e as autoridades receberão vários relatórios sobre o mesmo incidente.

Nesses casos, os controladores e a Autoridade Nacional na devem encontrar maneiras de garantir que as violações do processador sejam tratadas de forma eficiente. Para violações de vários clientes, pode ser sensato para os operadores fornecer uma notificação inicial à Autoridade Nacional, se eles e seus clientes concordarem. Essa abordagem permite que a Autoridade Nacional recebam informações em primeira mão sobre a situação também. A **Epeople** também pode preferir que o operador lide com os aspectos administrativos da notificação de assunto de dados, como cartas de impressão, instalação de sites informativos e call centers e organização de serviços de correção[1]. Se o operador for uma entidade conhecida diretamente aos titulares dos dados pode até ser apropriado que a notificação seja feita pelo próprio operador[2].

Em situações de violação de vários clientes, essa abordagem é claramente mais eficiente para

[1] Os operadores também preferem supervisionar esses aspectos da resposta, já que podem economizar dinheiro e garantir qualidade do serviço

[2] Se o operador não for conhecido diretamente pelo titular dos dados, a notificação deverá ser feita em nome do controlador para evitar confusão.

todos os participantes (inclusive os reguladores). No entanto, assim como ocorre na Europa, aqui no Brasil, dadas as potenciais penalizações associadas à não-conformidade com a LGPD, os controladores podem necessitar de uma orientação mais formal da Autoridade Nacional antes de permitirem que os seus operadores ajudem a cumprir as obrigações de notificação de violação.