REPORT

Resposta a Incidentes

Guidelines 9/2022 EDPB e a atuação fiscalizatória da ANPD em incidentes de segurança no Brasil

OPICE BLUM 25 anos
OPICE BLUM | BRUNO | VAINZOF

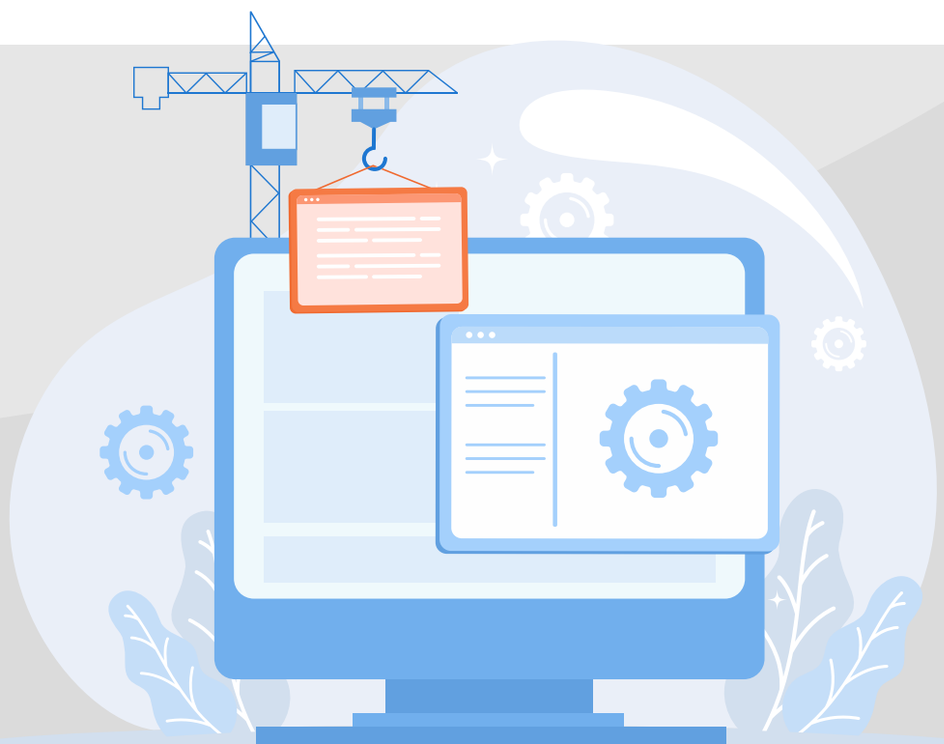
O **Regulamento Geral de Proteção de Dados da União Europeia** (*General Data Protection Regulation - GDPR*) prevê que uma violação de dados pessoais seja notificada à autoridade supervisora nacional competente (ou, no caso de violação transfronteiriça, à autoridade principal) e, em certos casos, que seja também comunicada aos indivíduos cujos dados pessoais foram afetados. A notificação é obrigatória para todos os controladores, a menos que seja improvável que da violação resulte risco aos direitos e às liberdades dos titulares. Os operadores também desempenham papel importante, devendo notificar qualquer violação ao seu controlador.

Em 3 de outubro de 2017, o *Working Party 29* (WP29) lançou diretrizes sobre o dever de notificação de violações envolvendo dados pessoais sob o **GDPR**, endossadas pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board - EDPB*) em sua primeira reunião **plenária**.

Agora, em 18 de outubro de 2022, o EDPB disponibilizou para consulta a versão **atualizada das diretrizes**, especificamente no que diz respeito ao parágrafo 73. O Conselho explica que notou a necessidade de clarificar os requisitos de notificação relativos às violações de dados pessoais em estabelecimentos não pertencentes à União Europeia, tendo, portanto, revisado e atualizado o parágrafo referente a esse assunto (enquanto o restante do documento foi mantido inalterado).

O parágrafo 73 das *Guidelines* passa a estabelecer que a mera presença de representante em um Estado-Membro da União Europeia não é suficiente para desencadear o mecanismo conhecido como "*one stop shop*" (OSS), que permite que uma organização lide com uma única autoridade supervisora líder ("*leader supervisory authority*" - LSA) para a maioria das atividades de tratamento. No entanto, a organização deve estar estabelecida na União Europeia e envolvida em **atividades transfronteiriças de tratamento**.

Com a alteração realizada no parágrafo 73 das Diretrizes, portanto, a violação deverá ser notificada a todas as autoridades dos Estados-Membros nos quais os titulares dos dados afetados residem. Essa notificação deve ser feita em cumprimento do mandado conferido pelo controlador ao seu representante, sendo responsabilidade do controlador.



A alteração afeta, desse modo, empresas brasileiras que realizam atividades transfronteiriças de tratamento de dados pessoais de titulares residentes na União Europeia, uma vez que terão de comunicar um incidente a diferentes autoridades de supervisão e, quando necessário, aos indivíduos afetados. Esse requisito soma-se ao já existente dever de notificar à Autoridade Nacional de Proteção de Dados (ANPD), a depender das circunstâncias e implicações do incidente, tema tratado a seguir.

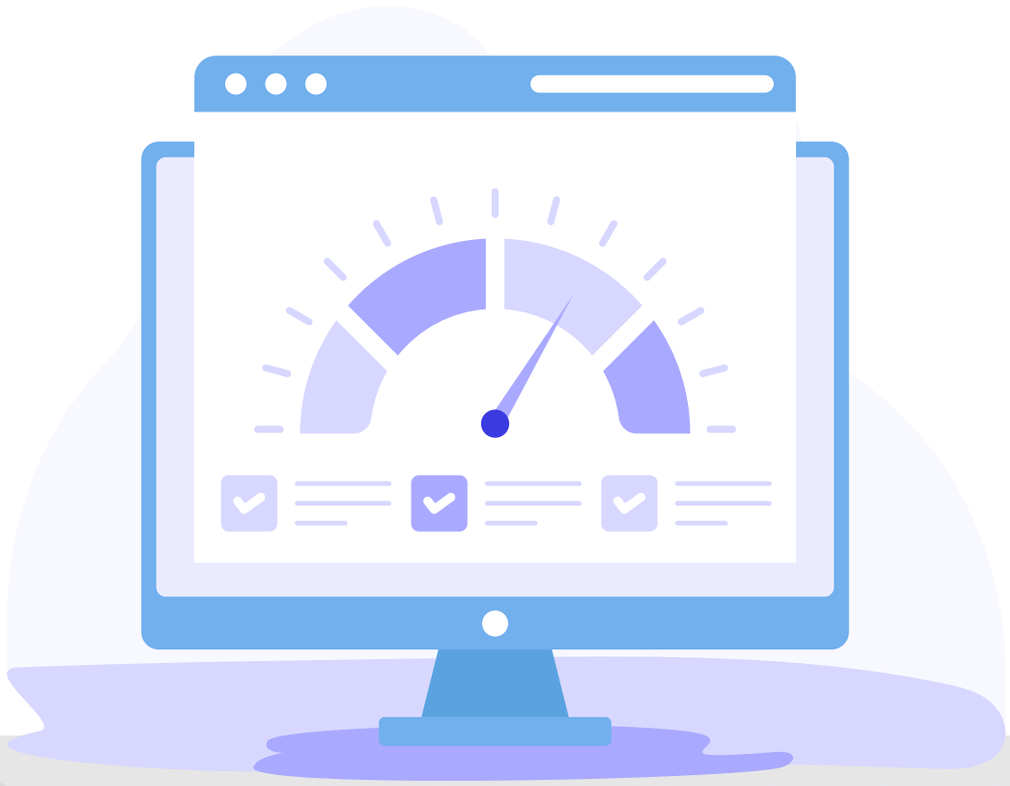
Nossa experiência lidando com incidentes de segurança ensina que, após a constatação da sua ocorrência, é preciso, inicialmente, buscar compreender qual base de dados pode ter sido comprometida, a fim de mapear se houve a exposição de dados pessoais e/ou de dados corporativos. Isso porque as estratégias de resposta e de contenção são diferentes em cada uma das situações.

Após a confirmação de que houve acesso indevido a dados pessoais, deve ser estudada a efetiva gravidade do incidente, por meio da elaboração do seu *score*. Embora inexista metodologia única, para traçar esse score com segurança, é necessário avaliar ao menos três pontos fundamentais:

- **Contexto do incidente:** entender quais tipos de dados foram comprometidos, se pessoais, sensíveis ou financeiros, entendendo o grau de exposição do titular diante de cada situação;

- **Facilidade/dificuldade** de identificação do titular a partir dos dados expostos;

- **Circunstâncias do incidente:** identificar em qual ponto houve comprometimento da segurança - confidencialidade, integridade ou disponibilidade - e se houve intenção maliciosa.



A partir do resultado, será possível confirmar se os titulares afetados e a ANPD devem ou não ser notificados, uma vez que a Lei Geral de Proteção de Dados (Lei 13.709/2018 – LGPD) determina que caberá ao controlador comunicar o incidente à ANPD e ao titular de dados sempre que dele resultar risco ou dano relevante aos titulares (art. 48). Em se tratando de operador, deverá ser realizada, assim, a comunicação tempestiva ao controlador, para que ele possa prosseguir com a notificação à Autoridade Nacional de Proteção de Dados e aos titulares, desde que haja risco ou dano relevante. Essa probabilidade será maior sempre que o incidente envolver: dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, gerando danos materiais ou morais, como discriminação; violação do direito à imagem e à reputação; fraudes financeiras; e roubo de identidade.

Note-se que, diferentemente do que ocorre na União Europeia, a ANPD tem adotado a postura de exigir a comunicação do incidente não somente a ela, mas também aos titulares, sempre que o controlador julgar haver risco ou dano relevante a eles. Como a própria Autoridade recomenda que os controladores sejam cautelosos, realizando a comunicação de forma clara e concisa, mesmo nos casos de dúvida sobre a relevância dos **riscos e danos**, pode acabar resultando em certa "fadiga informacional", com o titular recebendo comunicações constantes sobre incidentes, mesmo quando eles não tenham implicações relevantes.

A comunicação do incidente de segurança à ANPD deve conter, para além do previsto no § 1º do artigo 48 da LGPD, as seguintes informações:

- Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento, Encarregado de Proteção de Dados Pessoais (DPO – *Data Protection Officer*) ou outra pessoa de contato;

- Indicação se a notificação é completa ou parcial, destacando se a comunicação é preliminar ou complementar;

- Informações sobre o incidente de segurança de dados pessoais:

Data e hora da detecção

Data e hora do incidente e sua duração

Circunstâncias nas quais a violação de segurança de dados pessoais ocorreu, como perda, roubo, cópia, vazamento etc

Descrição dos dados pessoais e das informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados

Resumo do incidente, com indicação da localização física e meio de armazenamento

Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados

Medidas de segurança preventivas, técnicas ou administrativas, tomadas pelo controlador

Resumo das medidas implementadas para controlar os possíveis danos

Possíveis problemas de natureza transfronteiriça

Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir danos

Em relação ao prazo para notificação da ANPD e dos titulares, a LGPD determina que a seja feita em prazo razoável (art. 48, § 1º), definido pela Autoridade. Enquanto pendente a regulamentação, a autarquia recomenda que, após a ciência do evento adverso e havendo risco relevante, a comunicação aconteça com maior brevidade possível, de preferência dentro do prazo de dois dias úteis, contados da data do conhecimento do **incidente**.

Embora pendente de regulamentação, a observância do prazo indicado demonstra transparência e boa-fé do controlador, sendo considerada em eventual fiscalização pela ANPD. Além disso, a Autoridade pode requisitar do controlador cópia da comunicação realizada aos titulares afetados.

É importante destacar que, se tratando de comunicação preliminar, a Autoridade tem solicitado o envio de informações complementares no prazo de 30 dias corridos da comunicação inicial. Em caso de *ransomware*, é possível que a ANPD solicite também cópia do pedido de resgate dos dados.

Na prática, notamos cada vez mais a importância de se elaborar uma documentação minuciosa com a avaliação interna do incidente, as medidas tomadas e a já mencionada análise de risco, a fim de cumprir o princípio da responsabilização e da prestação de contas previsto no art. 6º, X, da LGPD. Isso porque a ANPD pode, no decurso do processo de investigação, solicitar ao controlador um relatório de tratamento do incidente de segurança.

Importante observar, também, que na Proposta do Regulamento de Dosimetria das Sanções aspectos de governança em privacidade e proteção de dados serão levados em conta para a mitigação das sanções, podendo chegar a 75% de redução. Por outro lado, a reincidência e o descumprimento de medidas orientativas ou preventivas emitidas pela Autoridade serão fatores agravantes.

Para saber mais sobre como identificar e reagir a incidentes de segurança, acesse **aqui** nossa cartilha sobre o tema. Com a iminente aprovação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas da **ANPD**, responder eficientemente a um incidente, preservando o máximo de evidências de sua ocorrência e de todas as medidas adotadas, torna-se ainda mais importante, inclusive para a mitigação de sanções. Demonstrar para a ANPD que a organização agiu com diligência para o entendimento do evento e a mitigação dos seus efeitos impactará de modo significativo na aplicação de eventual sanção.

Para mais informações, nossas equipes permanecem à disposição.

www.opiceblum.com.br | **contato@opiceblum.com.br**
Al. Joaquim Eugênio de Lima, 680, 1º andar, Jardim Paulista
CEP: 01403-000, São Paulo - SP, Brasil - Telefone: +55 (11) 2189-0061

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF