



POLÍTICA DE OCORRÊNCIA DE VIOLAÇÃO DE DADOS PESSOAIS

Considerando que, que a organização se preocupa com a proteção de dados pessoais e se propôs a cumprir o que determina o Regulamento Geral de Proteção de Dados, inclusive, no que tange a violação dos dados, estabelece os procedimentos internos para as tratativas nas hipóteses de ocorrência.

1. Ocorrências de violação de dados.

Nas hipóteses que configurarem qualquer indício de fraude, sabotagem, espionagem, desvio, falha, evento indesejado ou inesperado, que tenha probabilidade de comprometer ou ameaçar a segurança dos dados pessoais, são consideradas ocorrências de violação de dados.

Toda ocorrência de violação de dados deve ser tratada seguindo uma metodologia previamente definida pela organização, instituída na presente política.

O Gerenciamento de Incidentes de Segurança da Informação está voltado para proteger a informação e seus critérios de confidencialidade, integridade e disponibilidade. É uma metodologia organizada para gerir consequências de uma violação de segurança da informação, no intuito de minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

2. Procedimento diante da ocorrência

Em caso de violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, sempre que possível, o mais tardar 72 horas após ter tomado conhecimento dela, notificar a violação de dados pessoais à autoridade de controlo competente.

Caso a notificação à autoridade de controlo não seja feita no prazo de 72 horas, deve ser acompanhada dos motivos do atraso.

Caso a ocorrência seja percebida ou recepcionada pelo subcontratante, este notificará o responsável pelo tratamento, sem demora injustificada após tomar conhecimento de uma violação de dados pessoais. O responsável pelo tratamento, por sua vez, deve tomar as medidas cabíveis para notificar a autoridade de controle competente.

3. Teor da Notificação.

A notificação destinada a autoridade de controle competente deve conter, pelo menos:

- Descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares de dados em causa e as categorias e o número aproximado de registos de dados pessoais em causa;



- O nome dos dados de contacto do responsável pela proteção de dados ou outro ponto de contato onde possam ser obtidas mais informações;
- Descrição das prováveis consequências da violação de dados pessoais;
- Descrição das medidas tomadas ou propostas a serem tomadas pelo responsável pelo tratamento para fazer face à violação de dados pessoais, incluindo, se for caso disso, medidas para mitigar os seus possíveis efeitos adversos.

Quando o responsável não tiver as informações suficientes para apontar na notificação, no prazo de 72 horas, as informações podem ser fornecidas por fases, sem demora injustificada.

4. Comunicação ao titular

Quando a violação de dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunicará a violação de dados pessoais ao titular dos dados sem demora injustificada.

A comunicação ao titular dos dados deve descrever, em linguagem clara e simples, a natureza da violação de dados pessoais e conter, pelo menos, as informações e medidas que a organização adotou frente a ocorrência.

Constitui exceção a comunicação ao titular dos dados caso preenchida alguma das seguintes condições:

- O responsável pelo tratamento implementou medidas de proteção técnicas e organizacionais adequadas, e essas medidas foram aplicadas aos dados pessoais afetados pela violação de dados pessoais, em particular aquelas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como a criptografia;
- O responsável pelo tratamento tomou medidas subsequentes que garantem que o elevado risco para os direitos e liberdades dos titulares dos dados não é suscetível de se materializar;
- Envolver esforço desproporcional. Nesse caso, haverá, em vez disso, uma comunicação pública ou medida semelhante através da qual os titulares dos dados sejam informados de forma igualmente eficaz.

Se o responsável pelo tratamento ainda não tiver comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controle, tendo considerado a probabilidade de a violação de dados pessoais



resultar num risco elevado, pode exigir-lhe que o faça ou pode decidir que qualquer uma das condições referidas do parágrafo 3 sejam cumpridos.

5. Relato de ocorrências.

Em caso de violação de dados pessoais, o responsável pelo tratamento deve documentar quaisquer violações, incluindo os fatos relativos às ocorrências de violação de dados pessoais, bem como os seus efeitos e as medidas corretivas tomadas.