POLÍTICA DE

RESPOSTAS À INCIDENTES (LGPD)

POLI-0017-01

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-0017-01	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 Violações (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 **Epeople** está totalmente comprometida em proteger a segurança e a confidencialidade de todas as informações pessoais que nos são confiadas. Como parte desse compromisso, a **Epeople** documentou e implementou esta política de resposta a incidentes para orientar nosso tratamento interno de eventos e incidentes que podem impactar os "**Dados Pessoais",** que é qualquer informação que possa ser usada para identificar, localizar ou contatar um indivíduo, como um nome, um número de identificação, dados de localização, um identificador on-line ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física.

Uma **"Violação de Dados Pessoais"** significa uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma.

A **Epeople** define um **"Evento de Privacidade"** como qualquer ocorrência que possa comprometer a privacidade, confidencialidade, segurança ou integridade dos Dados Pessoais. Os Eventos de Privacidade incluem qualquer desvio das políticas de privacidade ou segurança da **Epeople** e, perda de Dados Pessoais, bem como qualquer uso não autorizado ou divulgação de Dados Pessoais.

Exemplos de evento de privacidade:

- Perda ou roubo de dispositivos contendo dados pessoais;
- Envio errado de e-mail, ou fax contendo dados pessoais;
- Presença de malware em um computador ou dispositivo contendo dados pessoais; e
- Transmissão de dados pessoais que não sejam permitidos pela política da **Epeople**.

A **Epeople** exige que todos os colaboradores e contratados relatem Eventos de Privacidade por meio de um processo estabelecido. Nós investigamos todos os Eventos de Privacidade, para

determinar o que aconteceu, estabelecer se algum dado pessoal foi comprometido e (em caso afirmativo) avaliar o risco de dano que poderia resultar da situação.

Em muitos casos, os Eventos de Privacidade não expõem de fato nenhum dado pessoal a nenhum indivíduo não autorizado. Por exemplo, os dados pessoais em um laptop perdido podem ter sido criptografados para que não possam ser visualizados por pessoas não autorizadas.

Em alguns casos, o Evento de Privacidade afeta os dados pessoais. Por exemplo, um dispositivo perdido pode conter informações não criptografadas. Ou um funcionário pode ter acidentalmente transmitido um arquivo contendo dados pessoais para o destinatário errado. Se o destinatário conseguiu visualizar os dados pessoais no arquivo, essa informação é uma divulgação não autorizada. Esses eventos são violações de dados pessoais.

Ao responder a violações de dados pessoais, é essencial que avaliemos com rapidez e precisão o risco de danos. Se os indivíduos estiverem em risco de sofrer danos ou risco, a política da **Epeople** é notificar os indivíduos o quanto antes e ajudá-los a mitigar os danos, bem como notificar a Autoridade Nacional.

Etapas de Avaliação

Todas as violações de dados pessoais devem ser avaliadas usando o seguinte processo de 3 etapas para determinar a resposta adequada da **Epeople**.

PASSO 1: Determinar se há um risco para os indivíduos que tiveram os dados violados como resultado do incidente.

Em caso afirmativo, a notificação dos indivíduos e da Autoridade Nacional deve ser feita dentro do prazo razoável e sem atrasos injustificados.

De modo geral, uma violação cria alto risco para um indivíduo quando, se não tratada, tal violação

pode ter um efeito prejudicial significativo sobre o indivíduo - por exemplo, resultar em discriminação, dano à reputação, perda financeira, perda de confidencialidade ou quaisquer outras desvantagens econômicas ou sociais significativas.

O risco tem de ser avaliado caso a caso, tendo em conta a circunstância do incidente e a natureza dos dados pessoais que foram comprometidos. Por exemplo, se elementos de dados sensíveis, como detalhes de contas bancárias, que poderiam colocar alguém em risco de crime financeiro forem perdidos, haverá um alto risco. Elementos de dados ainda menos sensíveis, como endereços de e-mail, podem resultar em alto risco, se a perda do elemento de dados colocar o indivíduo em risco de *phishing*. Por outro lado, a perda de um diretório pessoal contendo os tipos de elementos de dados encontrados nos cartões de visita dos colaboradores normalmente não resultaria em alto risco.

Da mesma forma, se os dados pessoais forem fortemente criptografados e as chaves de criptografia não forem comprometidas, é improvável que o incidente resulte em alto risco de danos.

Por uma questão de política, assumimos que existe um alto risco de dano se dados confidenciais não criptografados forem roubados. Também assumimos que existe um alto risco de dano se Dados Pessoais (como números de identificação nacional, número do CPF ou informações de conta financeira) ou Dados Pessoais Sensíveis tiverem sido transmitidos para um destinatário desconhecido ou não confiável.

Se houver um alto risco real de dano, os seguintes passos devem ser tomados imediatamente:

O tempo é essencial.

1. A **Epeople** precisa notificar a Autoridade Nacional assim que possível.

   a. *[Este aviso é feito, em regra, pelo Controlador de Dados.] Se aplicável e apropriado, a notificação também pode ser feita para (i) cumprimento da lei; (ii) outras agências reguladoras; (iii) equipes de fraude da* ***Epeople****; e (iv) a seguradora da* ***Epeople***.

2. A **Epeople** deve notificar o indivíduo afetado o mais rápido possível.

   a. A carta de notificação deve alertar aos indivíduos dos possíveis riscos e danos do vazamento, bem como os passos que os indivíduos devem seguir para minimizar os riscos.

   b. As cartas de notificação devem seguir integralmente todos os requisitos do art. 48 da LGPD, bem como quaisquer outros requisitos legais aplicáveis:

      - ✓ descrever a natureza da violação dos dados pessoais, incluindo, sempre que possível as categorias e o número aproximado de titulares de dados envolvidos e as categorias e o número aproximado de registro de dados pessoais envolvidos na violação;
      - ✓ comunicar o nome e os detalhes para contato do encarregado de proteção dos dados da empresa ou outro ponto de contato onde maiores informações podem ser obtidas;
      - ✓ descrever as consequências prováveis da violação de dados; e
      - ✓ descrever as medidas adotadas ou propostas pelo controlador para tratar da violação de dados pessoais, incluindo, quando apropriado, medida para mitigar os riscos e prejuízos já causados.

   c. Se não for possível enviar cartas em tempo hábil, a **Epeople** deve considerar maneiras alternativas de proceder com a notificação dos indivíduos afetados. Como por exemplo, a **Epeople** pode publicar um aviso sobre o incidente na página inicial de seu site e enviar informações sobre o incidente para as pessoas por e-mail.

3. A **Epeople** deve, se apropriado, notificar outras autoridades, dependendo da situação. Por exemplo, se os titulares dos dados estiverem localizados em vários países a **Epeople** deve notificar as autoridades relevantes de proteção de dados desses países para que possam fornecer o suporte apropriados aos indivíduos.

4. Se a violação não lhe parecer de alto risco par os direitos e liberdades de um indivíduo, vá para a o passo 2.

PASSO 2: Determinar o nível de risco para os indivíduos impactados.

Se existir risco de dano é necessária a notificação da Autoridade Nacional, assim que possível.

Use o Scorecard de Resposta a Incidentes anexado abaixo para avaliar o risco de dano com base em fatores estabelecidos que determinam a probabilidade de risco caso os Dados Pessoais tenham sido comprometidos.

Se a pontuação gerada pelo Scorecard de Resposta a Incidentes for 4 ou menor, há um baixo risco de dano aos indivíduos. (Mova para o passo 3.)

Para completar esta análise, a **Epeople** deve considerar (1) os elementos de dados específicos que foram expostos, (2) os países de residência dos indivíduos impactados e, se aplicável, (3) a legislação específica do país ou orientação nacional. O DPO concluirá essa análise.

Se a segurança, confidencialidade, a integridade dos dados pessoais tiverem sido comprometidos (por exemplo, o score for de 5 ou mais), há um risco de dano.

PASSO 3: Documente que não há risco de dano a indivíduos que exija a notificação deles ou da Autoridade Nacional.

Manter a documentação referente à investigação de acordo com o documento da AS Contábil política de retenção.

Quando as notificações individuais não são necessárias para alertar as pessoas, haja vista a ausência de risco ou de dano, a **Epeople** não efetuará a notificação, seja dos indivíduos, seja da Autoridade

Nacional.

A **Epeople** está empenhada em garantir que os interesses dos indivíduos sejam protegidos em conexão com incidentes de segurança. Nossa política é notificar reguladores e indivíduos (e fornecer correção adequada) sempre que os indivíduos tiverem qualquer risco real de dano como resultado de nossos erros - independentemente de haver qualquer obrigação legal de notificá-los.

A **Epeople** compromete-se a cumprir os requisitos legais aplicáveis, que algumas vezes exigem notificação de violação mesmo quando não há risco de dano. Sempre forneceremos notificação de violação conforme exigido por lei. Cooperaremos com a Autoridade Nacional caso determine que a notificação é necessária mesmo que o risco de dano seja moderado ou baixo.

O artigo 48 da LGPD determina que a notificação só deva existir quando a violação puder acarretar risco ou dano ao indivíduo. Este artigo reflete a visão da política pública de que os indivíduos não devem ficar desnecessariamente alarmados com eventos que não os puseram em risco ou danos.

Se qualquer pessoa estiver em dúvidas sobre a segurança das informações a **Epeople** irá sanar as dúvidas.

A **Epeople** mantém registros de todas as investigações de incidentes de privacidade por um período mínimo de cinco (5) anos ou mais, caso determinado pela Autoridade Nacional. Para tanto, é necessário que esse registro contenha cópias de sua documentação (incluindo o Scorecard de Resposta a Incidente preenchido e quaisquer modelos de carta de notificação) para retenção.

Scorecard de Respostas a Incidentes

A **Epeople** avalia todos os incidentes para determinar se existe a ocorrência de incidente de segurança que possa acarretar risco de que os dados pessoais tenham sido comprometidos ou que indivíduos tenham se tornados vulneráveis ao risco de danos.

Levamos em conta 4 fatos que devem ser considerados para determinar o risco de dano. Esses fatores são:

- ✓ A natureza e a extensão dos dados pessoais envolvidos, incluindo os tipos de dados identificadores e a probabilidade de re-identificação dos indivíduos;
- ✓ A pessoa não autorizada que usou os Dados Pessoais ou para quem a divulgação foi feita;
- ✓ Se os dados pessoais foram realmente adquiridos ou visualizados; e
- ✓ Até que ponto o risco para os dados pessoais foi mitigado.

Dados Pessoais (DP) pode ser definido como: Qualquer informação relativa a uma pessoa singular identificada ou identificável ("titular de dados"); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador on-line ou a um ou mais fatores específicos da física, fisiológica, identidade genética, mental, económica, cultural ou social dessa pessoa singular.

Qualquer informação (sozinha ou quando usada em combinação com outras informações dentro do controle direto da **Epeople**) pode ser usada para identificar, localizar ou contatar um indivíduo, juntamente com todas as informações relacionadas a esse indivíduo.

Os Dados Pessoais incluem todos os Dados Pessoais Sensíveis e outras informações óbvias, como nome da pessoa ou endereço de e-mail, bem como informações menos óbvias, como qualquer endereço IP ou dados biométricos, se tais dados pudessem possivelmente estar associado a um indivíduo.

Os dados pessoais podem estar em qualquer mídia ou formato, incluindo registros informatizados ou eletrônicos, bem como arquivos em papel.

Dados Pessoais Sensíveis (DPS) também são regulados pela lei. DPS são um subconjunto dos DP, que devido à sua natureza foram classificados por lei ou política como merecendo proteção adicional de privacidade e segurança. Dados Pessoais Sensíveis consistem em (a) raça ou origem étnica, (b) opiniões políticas, (c) religião, (d) associação a sindicatos, (e) vida sexual ou orientação sexual, (f) saúde física ou mental, e (g) acusações criminais ou registros relacionados a crimes e alegações de crimes.

O scorecard abaixo nos permite avaliar o risco de danos ao indivíduo de uma violação de dados pessoais. Este documento deve ser anexado *ao Relatório de Ocorrência*.

1. A natureza e a extensão dos dados envolvidos, incluindo os tipos de dados identificadores vazados e a probabilidade de re-identificação:

0. Baixo risco	1. Risco possível	2. Alto risco
DP mas não DPS e/ ou baixo risco de associação	DP associado a um individuo (mas não DPS)	Dados não criptografados
Por exemplo: nome individual associado a informações públicas (endereço postal, nome da empresa ou título) ou dados demográficos Qualquer DP ou DPS se criptografado usando uma criptografia padrão do setor, desde que as chaves de criptografia não sejam comprometidas	Nome individual associado a quaisquer outros tipos de dados pessoais, como endereço de e-mail ou número de telefone, histórico de compras, detalhes de emprego ou informações sobre salários	Identificadores emitidos pelo governo Números de conta financeira individuais Credenciais da conta de usuário (endereço de e-mail e senhas, perguntas / respostas de segurança)

ESSE EVENTO: Circule a pontuação referente a esse evento: 0 1 2

EXPLICAR:_____

_____

_____

_____

_____

2. Pessoa não autorizada que usou o DP ou para quem a divulgação foi feita:

0. Baixo risco	1. Risco possível	2. Alto risco
Destinatário confiável	Destinatário digno de confiança	Destinatário não confiável
Funcionário da empresa Fornecedor da empresa Parceiro de negócios da empresa Agência governamental	Terceiro com a qual a empresa não tenha relação contratual, mas que fornece garantias confiáveis de que os dados não serão utilizados de maneira incorreta (por exemplo, um antigo fornecedor ou cliente). Uma entidade regulamentada, como uma instituição financeira, companhia de seguros ou prestador de serviços de saúde	Destinatário desconhecido Destinatários com intenção maliciosa conhecida ou suspeita (por exemplo, roubo de dados)

ESSE EVENTO: Circule a pontuação referente a esse evento: 0 1 2

EXPLICAR

_____

_____

_____

_____

3. Se os DP foi visto ou coletado:

0. Baixo risco	1. Risco possível	2. Alto risco
Não visto e não coletado	Visto (ou parcialmente visto) mas não coletado	Coletado
A empresa constata que o arquivo foi enviado para o destinatário errado e recupera os dados antes de serem acessados O dispositivo / mídia perdidos é recuperado e a análise forense demonstra que os dados não foram acessados	O destinatário abre o pacote ou o arquivo, mas percebe que ele foi direcionado incorretamente e exclui (devolve ou destrói) o arquivo sem usar ou divulgar ainda mais as informações	A empresa não foi capaz de recuperar os dados

ESSE EVENTO: Circule a pontuação referente a esse evento: 0 1 2

EXPLICAR:

_____

_____

_____

_____

4. Até que ponto o risco do titular dos DP foi mitigado:

0. Baixo risco	1. Risco possível	2. Alto risco
A empresa, de boa-fé, tem razões para acreditar que esse DP não foi e não será usado, divulgado ou retido.	A empresa, de boa-fé, tem razões para acreditar que o DP não foi e não será usada ou divulgado.	Sem mitigação

DP foi totalmente recuperado. O destinatário confiável ou digno de confiança forneceu garantias por escrito confiáveis de que os dados não foram usados ou divulgados e que nenhuma instância dos dados foi retida. Os DP foi criptografado e as chaves de criptografia não foram comprometidas.	OS DP foram recuperados do sistema do receptor. O destinatário confiável ou digno de confiança forneceu garantias por escrito confiáveis de que os dados não foram usados ou divulgados (mas pode ocorrer retenção nas cópias de segurança). O destinatário confiável ou digno de confiança estabeleceu um programa para proteger informações semelhantes internamente.	A empresa não tem garantias quanto ao uso, divulgação ou retenção do DP

ESSE EVENTO: Circule a pontuação referente a esse evento: 0 1 2

EXPLICAR:

_____

_____

_____

_____

5. Quaisquer outros fatores ou informações que possam ajudar a determinar o tipo de dano:

EXPLICAR:

_____

_____

_____

_____

Calcular a Pontuação

Adicione a soma de pontuação da avaliação de risco total dos fatores 1-4 acima.

Pontuação total 7 ou 8: A violação de dados pessoais coloca os indivíduos em alto risco de danos. A ANPD e os indivíduos afetados devem ser notificados o mais breve possível.

Pontuação total 5 ou 6: A violação de dados pessoais cria um risco de dano. O Controlador [ou DPO] deve notificar a ANPD para determinar se a notificação dos titulares de dados é garantida. Se o incidente incluir elementos de dados que acionam leis de notificação de violação em outros países, a notificação provavelmente será necessária.

Pontuação total 4 ou menor: não há ou há um risco muito baixo de dano. Embora você possa ter um ou dois fatores de alto risco (como DP sensível em um dispositivo roubado), a probabilidade de comprometimento deve ser baixa (por exemplo, se os dados estiverem criptografados). O risco também pode ser baixo se os dados foram visualizados por um terceiro confiável com a atenuação apropriada do evento.

Pontuação Total: _____