Política de Gestão de Crise em incidentes de Segurança com Dados Pessoais

GP-QA-007_pt

Controle de revisões					
Revisão	**Data**	**Seção afetada**	**Elaborado**	**Revisado**	**Aprovado**
01	20/03/23	inicial	M.Pinheiro	M.Pinheiro	M.Messias

Sumário

1. INTRODUÇÃO

Essa Política de Gestão de Crise em Incidentes de Segurança com Dados Pessoais foi elaborada levando em consideração a governança em proteção de dados pelo GRUPO ADAPTS instituída após a vigência da Lei Geral de Proteção de Dados brasileira, a Lei nº 13.709/2018.

2. OBJETIVO

Essa Política tem vigência imediata a todos os colaboradores do GRUPO ADAPTS e tem por finalidade em conjunto com demais normativos internos da Fundação normatizar procedimentos reativos diante de um incidente de proteção de dados pessoais ainda que suspeito.

A governança em proteção de dados pessoais envolve, além da adoção de medidas preventivas a ocorrência de incidentes ou irregularidades no tratamento de dados pessoais das pessoas físicas com quem o GRUPO ADAPTS mantenha relacionamento, a adoção de medidas mitigadoras de risco à direitos e liberdade de titulares após um incidente de segurança envolvendo dados pessoais.

Esse documento poderá ser alterado a qualquer momento de acordo com a evolução da maturidade de governança em proteção de dados pessoais ou até mesmo diante de alterações legislativas sobre a matéria e novas regulamentações da Autoridade Nacional de Proteção de Dados ou outra agência reguladora.

3. GLOSSÁRIO

Para melhor compreensão da Política apresentada, disponibilizamos o glossário abaixo:

ANPDA Autoridade Nacional de Proteção de Dados

DADOS PESSOAIS Dados que identifiquem ou possam identificar uma pessoa natural.

DADOS PESSOAIS COMUNS Por exclusão, dados pessoais que não sejam sensíveis ou de criança e adolescente (exemplo: nome, CPF, e-mail, salá- rio, patrimônio).

DADOS PESSOAIS SENSÍVEIS Dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organiza- ção de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

DADOS PESSOAIS DE CRIANÇA E ADOLESCENTE Dados pessoais de menores de 18 anos, independente se dados comuns ou sensíveis.

DADOS PESSOAIS CADASTRAIS Dados pessoais objetivos como nome, CPF, endereço, tele- fone, e-mail etc.

DADOS PESSOAIS COMPORTAMENTAIS Dados pessoais que revelem comportamentos e preferências (exemplo, gosto por músicas, preferências de lazer).

DADOS PESSOAIS INFERIDOS Dados pessoais supostos pela empresa após análises e combinações de outros dados pessoais coletados.

INCIDENTE EM SEGURANÇA DE DADOS PESSOAIS Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS Pessoa indicada pelo controlador para atuar como canal de comunicação entre a empresa, os empregados e a Autoridade Nacional de Proteção de Dados.

TRATAMENTO DE DADOS PESSOAIS Qualquer ação que envolva dados pessoais, desde coleta, compartilhamento, armazenamento, acesso, cruzamento, etc.

CONTROLADOR DE DADOS PESSOAIS Empresa que trata dados pessoais e a quem compete a decisão sobre o tratamento. Um dos dois tipos de agente de tratamento de dados pessoais.

OPERADOR DE DADOS PESSOAIS Empresa que trata dados pessoais a mando de outra e atendendo a regras de outra. Um dos dois tipos de agente de tratamento de dados pessoais.

LGPD Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

TRANSFERÊNCIA INTERNACIONAL Compartilhamento de dados coletados no Brasil com pes- soa jurídica no exterior.

4. PAPÉIS E RESPONSABILIDADES

Dada a relevância em governança de dados pessoais para o GRUPO ADAPTS, compete a qualquer colaborador, além da prevenção de irregularidades e adoção de condutas adequadas ao tratamento de da- dos pessoais em conformidade com a Lei Geral de Proteção de Dados e melhores práticas, identificar e comunicar de imediado a supeita ou ocorrência de incidentes de segurança em dados pessoais.

Qualquer colaborador que tomar conhecimento acerca da ocorrência ou iminência de incidente relacionados a segurança da informação deverá comunicar ao setor de Segurança da Informação, que envolverá o Encarregado pelo Tratamento de Dados Pessoais, para apuração do envolvimento, no incidente ou suspeita de incidente, de dados pessoais bem como a ocorrência de riscos de dano ou dano efetivo a direitos e liberdades de titulares.

Uma vez apurado o envolvimento de dados pessoais, no incidente de segurança da informação, o Encarregado pelo Tratamento de Dados Pessoais deverá iniciar o procedimento de resposta em quatro etapas: Avaliação, Comunicação, Mitigação e Apuração de Responsabilidades e Melhoria Contínua.

Após a avaliação preliminar, havendo indícios de envolvimento no incidente de risco de dano

ou dano efetivo a direitos e liberdades de titulares, a Diretoria deverá ser comunicada pelo Encarre- gado pelo Tratamento de Dados Pessoais e em conjunto deliberar por: 1) constituir um Comitê de Crise com a presença da Presidência e Diretoria, Encarregado pelo Tratamento de Dados Pessoais, membro da Segurança da Informação, membro de área estratégicas cuja ocorrência do incidente foi identificada; 2) contratar empresa especializada de investigação, em especial se o incidente for no ambiente digital e envolver cibersegurança; 3) contratar empresa especializada para assessorar as comunicações oficiais aos agentes fiscalizadores e/ou titulares; 4) acionar assessoria de imprensa se for necessário posicionamento reativo ou espontâneo na mídia.

5. PROCEDIMENTOS

5.1 Avaliação

Após a ocorrência do incidente de segurança em dados pessoais ou suspeita da ocorrência de incidente de segurança será necessário avalia-lo, verificando a natureza, categoria, quantidade de titulares de dados afetados e consequências concretas e prováveis a direitos e liberdades dos titulares.

5.1.1 A avaliação preliminar sobre a ocorrência do incidente deve visar:

A) Apuração da suspeita ou denúncia de incidente em segurança de dados pessoais para confirmar a ocorrência do evento;

B) Adoção de medidas preliminares de contenção dos danos e interrupção do incidente em seguran-ça de dados pessoais;

C) Levantamento de informações como:

(I) identificação da data e hora do incidente e sua duração;

(II) circunstâncias em que ocorreu a violação de segurança de dados pessoais;

(III) descrição dos dados pessoais (categorias, se dados pessoais comuns, cadastrais, inferidos ou dados sensíveis ou dados de criança e adolescente) e informações afetadas;

(IV) indicação da localização física e meio de armazenamento, identificação do banco de dados violados ou ativo de informação atacado. Recomenda-se a pesquisa no Mapa de Banco de Dados;

(V) identificação da forma de proteção dos dados pessoais violados, se in natura

ou protegido por senha ou qualquer outra ferramenta. Recomendamos pesquisar no Relatório de Operações de Tratamento;

(VI) identificação da categoria de pessoas físicas envolvidas e possíveis consequências e efeitos negativos sobre esses titulares dos dados afetados. Recomenda-se a pesquisa no Mapa de Pes- soas Físicas Relacionadas;

(VII) identificação, dentre os dados pessoais que foram objeto do incidente, se estão envolvidos em operações de tratamento em que o GRUPO ADAPTS é controladora ou operadora;

(VIII) avaliação sobre a necessidade de contratação de serviços especializados de investigação e/ou resposta ao incidente.

5.2 Comunicações obrigatórias

5.2.1 A responsabilidade de comunicação à ANPD e ao titular, conforme previsão do art. 48 da LGPD é do controlador de dados, sendo assim, cabe a Grupo adapts identificar a sua posição na operação de tra- tamento cujos dados pessoais foram objeto do incidente de segurança. Recomenda-se pesquisar no Relatório de Operações de Tratamento para identificação dessa posição enquanto agente de tratamento de dados.

5.2.2 Caso o GRUPO ADAPTS seja operadora de dados, deverá notificar, dentro do prazo previsto no contrato, o controlador com quem mantem relação que lastrei o compartilhamento dos dados pessoais envol- vidos no incidente. Na ausência de previsão no contrato sobre o prazo para promover essa notificação, recomenda-se realizá-la em, no máximo 48 (quarenta e oito) horas;

5.2.3 Caso o GRUPO ADAPTS seja controladora de dados, deverá:

a) Avaliar o existência de risco de dano ou dano efetivo a direitos dos titulares com o incidente para apurar a obrigatoriedade em promover a comunicação à Autoridade Nacional de Proteção de Dados.

Considerando que não há na lei e em regulamentos brasileiros o apontamento das hipóteses em que a comunicação à ANPD seja obrigatória, recomenda-se utilizar como parâmetros considerados isoladamente identificadores da obrigatoriedade de comunicação à ANPD: (I) o

envolvimento, no incidente, de dados pessoais sensíveis; (II) o envolvimento, no incidente, de dados pessoais de crianças e adolescentes; (III) o envolvimento, no incidente, de alto volume de dados pessoais; (IV) quando o incidente tiver o potencial de ocasionar danos materiais ou morais.

Em caso de a comunicação à ANPD ser obrigatória deverá ser realizada, pelo Encarregado pelo Tratamento de Dados Pessoais, por meio de formulário eletrônico padrão elaborado pela ANPD, disponível em https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-inci- dentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx, e enviar por meio de peticionamento online no portal do Governo Federal no endereço https://www.gov.br/secretariageral/pt-br/sei-peti- cionamento-eletronico.

A comunicação deverá ser realizada no prazo de até 2 (dois) dias úteis contados da data do conhecimento do incidente.

As informações necessárias à comunicação à ANPD estão descritas no formulário e devem conter:

a) identificação do controlador (GRUPO ADAPTS), a identificação e dados de contato do Encarregado pelo Tratamento de Dados Pessoais;

b) indicação se a notificação é completa ou parcial e sendo parcial, indicação de que se trata de comunicação preliminar ou complementar;

c) informações sobre o incidente de segurança com dados pessoais, resumo do incidente de

d) segurança com dados pessoais;

e) identificação de medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador;

f) resumo das medidas implementadas até o momento para controlar os possíveis danos, possíveis problemas de natureza transfronteiriça;

g) outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos;

h) todas as informações listadas no item 5.1 desta Política.

5.2.4 A comunicação deve ser realizada ainda que não seja possível conhecer todas as informações requisitadas pela ANPD, podendo ser realizada em fases conforme apuração de todas as informações envolvidas no incidente de segurança em dados

pessoais.

5.3 Mitigação do risco e apuração de responsabilidades

5.3.1 Após a confirmação e avaliação preliminar do incidente em segurança de dados pessoais, é in- dispensável apurar as causas a fim de que sejam adotadas medidas de mitigação do risco verificado bem como apurar a responsabilidade sobre o incidente.

5.3.2 Para a identificação da causa bem como a responsabilidade, poderá haver uma investigação interna a ser realizada por um grupo de trabalho designado ou poderá ser contratado serviço espe- cializado para a apuração da responsabilização.

5.3.3 A identificação da causa implicará a alteração de medidas de prevenção que deverão ser trabalhados dentro de um programa de melhoria contínua.

5.3.4 A investigação da responsabilidade a fim de apurar autoria e intenções, se criminosas ou não, é um procedimento obrigatório a ser desenvolvido pelo GRUPO ADAPTS ou, se for o caso, da suspeita de uma ação criminosa que seja noticiada as Autoridades Policiais competentes.

5.3.5 Caso seja identificada a autoria do incidente por um colaborador da GRUPO ADAPTS, deverá ser aberta sindicância trabalhista para comprovação e reunião de documentos que lastrem a deliberação acerca da aplicação de sanções.

5.3.6 Todas as medidas adotadas para apuração da causa e identificação da responsabilização deverão ser documentadas em relatório específico de produção interna.

5.4 Melhoria contínua

5.4.1 5A Lei Geral de Proteção de Dados prevê, no artigo 50, o programa de governança em privacida- de que demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais.

5.4.2 Tal programa deverá ser aplicável a todo o conjunto de dados pessoais que esteja sob controle do GRUPO ADAPTS e adaptado à estrutura, escala e volume de suas

operações, bem como à sensibilidade dos dados tratados.

5.4.3 Para tanto o GRUPO ADAPTS deve estabelecer políticas e salvaguardas adequadas com base em um processo de avaliação sistemática e constante dos impactos e riscos à privacidade no tratamento de dados pessoais em cada setor do seu Organograma.

5.4.4 Uma ocorrência de incidente em segurança de dados pessoais deve, necessariamente, gerar a adoção de novas medidas de proteção e treinamento da equipe de colaboradores e, eventualmente, operadores de dados pessoais envolvidos na cadeia da operação de tratamento.

6. CONCLUSÃO

6.1.1 Esta Política de Gerenciamento tem como propósito servir de referência para o planejamento e execução de medidas durante os possíveis cenários de crise. Ela poderá ser utilizada também como insumo para o treinamento e preparo dos colaboradores do GRUPO ADAPTS.

6.1.2 Ressalte-se que esta Política não tem a pretensão de apresentar uma descrição ampla das estratégias de gerenciamento de crises, mas padronizar processos, delimitar fases, ações e papeis dos envolvidos e, assim, evitar ruídos e conflitos, inserindo o GRUPO ADAPTS em um alto patamar de preparação para situações de instabilidade em proteção de dados pessoais.

Salvador, 28 de maio de 2021

grupo adapts

Manoel Messias
Gerente Geral Grupo Adapts