Fundação Euclides da Cunha

Política de gestão de incidentes com dados pessoais

versão 1.0

Histórico de versões

Versão	Data	Observações
0.1	17/09/2024	Versão inicial, elaborada pelo Comitê de Privacidade
0.2	18/09/2024	Validação da Alta Gestão
0.3	02/10/2024	Validação da Assessoria Jurídica
1.0	01/11/2024	Revisão final e 1ª versão publicada

Fundação Euclides da Cunha

Índice

1. Introdução

Esta Política de Gestão de Incidentes com Dados Pessoais da FEC foi construída como parte dos esforços de adequação da FEC à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD).

O objetivo desta Política é estabelecer diretrizes sobre o que deve ser feito em caso de incidentes com dados pessoais sob o controle e tratamento da FEC.

Importante salientar que a gestão de incidentes deve se dar para quaisquer eventos ocorridos em meios digitais e não digitais, não havendo distinção na forma de condução.

Por fim, cabe reforçar que esta política destina-se a tratar apenas incidentes que envolvam dados pessoais e que, portanto, estejam no escopo da LGPD.

2. Definições

ANPD:

É a Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Dado pessoal:

Informação relacionada a pessoa natural que permita de qualquer forma a identificar;

Encarregado(a) de dados:

Pessoa nomeada pela Alta Gestão da FEC em ato específico, para atuar como canal de comunicação entre a FEC, os titulares dos dados e a ANPD.

Incidente:

Desvio ou violação de procedimento de trabalho que resulte em acesso, divulgação, alteração, supressão ou qualquer outro tratamento não autorizado de dados pessoais.

Notificador:

Pessoa física ou jurídica que comunique, mesmo que anonimamente, um incidente com dados pessoais.

Titular:

A pessoa física a quem se refere um ou mais dados pessoais. Pode ser entendida como a “proprietária” dos dados.

Tratamento de dados:

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

3. O que são dados pessoais?

A LGPD define que dado pessoal é informação relacionada a pessoa natural identificada ou identificável. Isto quer dizer que todo dado que permite identificar, direta ou indiretamente, uma pessoa é um dado pessoal.

Alguns exemplos de dados pessoais: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, informações bancárias, cartão de crédito, fotografia, prontuário de saúde, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.

Dentro da categoria de dados pessoais, há os que a LGPD considera dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

4. O que é um incidente?

Conforme menciona a definição acima, todo e qualquer desvio em relação ao tratamento dos dados pessoais pode ser um incidente. Dito de outra forma, um incidente é um evento em que o fluxo normal definido acaba não sendo seguido.

Alguns exemplos de incidentes:

- Um e-mail que foi enviado por engano para algum setor ou pessoa;
- Um documento impresso esquecido ou deixado em local inadequado;
- Um processo de pagamento de pessoa física enviado para uma área diferente da que deveria ter sido;
- Um sistema que exibe informações pessoais para outros usuários que não deveriam vê-las.

Incidentes como os exemplificados acima, quando ocorrem apenas dentro da própria instituição, não são considerados graves, pois as autorizações são dadas pelos titulares dos dados para a instituição, a FEC como um todo, não apenas para um colaborador ou setor específico. Logo, se um setor da FEC que não deveria acessar os dados o faz, isto ainda está protegido pela autorização obtida.

Apesar disso, é importante compreender que estes ainda são incidentes, e devem ser tratados para evitarmos que ocorram novamente ou que se agravem no futuro.

5. Vazamento de Dados Pessoais

Como vimos, a definição de incidente é bastante ampla. Entretanto, quando um incidente envolve **alguém externo à FEC**, que indevidamente tem acesso a dados pessoais não autorizados, isto caracteriza um tipo específico de incidente chamado **Vazamento de Dados Pessoais**.

O vazamento de dados pessoais é, portanto, um tipo mais grave de incidente, pois envolve agentes de fora da Fundação, o que exigiria autorização prévia do titular dos dados pessoais.

Só quem pode autorizar o acesso aos dados pessoais é o titular destes dados, ou seja, somente a pessoa a quem estes dados se referem.

Alguns exemplos de vazamentos:

- Envio de informações de um bolsista para outra pessoa do mesmo projeto, por engano;
- Envio de informações sobre pessoas de um projeto, para coordenador ou secretaria de outro projeto.

6. Quem é responsável por tratar os incidentes?

A **FEC**, conforme determina a LGPD, possui uma pessoa designada como **Encarregado(a) de Dados**. Esta é a pessoa responsável por coordenar o registro, investigação, tratamento e comunicação de todos os incidentes. É o Encarregado de Dados quem determina, de acordo com a gravidade do incidente, que medidas devem ser adotadas, desde um simples registro do ocorrido e orientação aos envolvidos para prevenir futuras ocorrências, até a abertura de procedimentos mais complexos de investigação e comunicação aos titulares e autoridades, em caso de vazamentos e ocorrências mais sérias.

Além do Encarregado de Dados, a FEC possui um **Comitê de Privacidade**, um grupo interdisciplinar de pessoas responsáveis pela implementação das adequações necessárias da Fundação à LGPD, incluindo a construção de procedimentos, normas internas e políticas, como esta, de tratamento de incidentes. Este Comitê pode ser acionado pelo(a) Encarregado de Dados para realizar as atividades relativas ao tratamento dos incidentes, quando necessário.

7. Processo de tratamento de incidentes

O tratamento dos incidentes poderá variar conforme sua gravidade, mas tudo se inicia com a identificação de um incidente e se divide nas seguintes fases: Identificação; Análise; Resposta e Registro.

1. Identificação

Tudo começa quando alguém identifica um incidente. Toda e qualquer pessoa física ou jurídica, inclusive de fora da FEC, pode identificar um incidente a partir da observação das informações que envia ou recebe, e dos procedimentos que deveriam acontecer.

Alguns exemplos de identificação de incidentes são:

- Um colaborador de um dado setor da FEC recebe um e-mail que não deveria ter sido enviado a ele(ela) ou ao seu setor;
- Alguém encontra um documento contendo informações pessoais, deixado em uma mesa ou espaço comum na sede da FEC;
- Um colaborador recebe por engano o contracheque de outra pessoa.
- Alguém envia por engano um atestado médico para um setor diferente que não a GRH.
- Um coordenador de projeto recebe informações sobre uma pessoa que não é membro do seu projeto;

Uma vez que alguém identifique um potencial incidente, é crucial que ele seja imediatamente notificado para o(a) Encarregado de Dados através do e-mail a seguir:

encarregado.dados@somosfec.org.br

Para auxiliar no processo de análise do incidente, é importante inserir todas as informações disponíveis sobre o ocorrido e comunicar com a maior brevidade possível!

2. Análise

A partir do momento em que o(a) Encarregado de Dados recebe uma notificação de incidente, faz-se uma análise inicial para determinar:

- Há informações pessoais envolvidas?
- Quem são as pessoas/ setores envolvidos?
- Há alguma pessoa externa à FEC envolvida?

Com isto respondido, o(a) Encarregado de Dados toma a decisão de reunir ou não o Comitê de Privacidade para uma análise mais aprofundada do incidente. Neste momento também já se inicia a fase de registro, com a coleta destas primeiras informações.

Após isto, com ou sem a ajuda do Comitê de Privacidade, será realizada uma análise mais detalhada do incidente, que vai responder às seguintes questões:

a. Quando ocorreu o incidente?
b. Qual a cadeia de eventos (linha do tempo) que levou ao incidente?
c. Houve vazamento de dados?
d. Há dados pessoais sensíveis envolvidos?
e. Qual a criticidade (alta, média ou baixa) do incidente e por quê?
f. Existe necessidade de comunicação ao titular dos dados ou à ANPD?
g. Quais desvios aconteceram nos procedimentos para que o incidente ocorresse?
h. Que ações a FEC pode adotar para prevenir novos incidentes como este?

Para realizar esta análise diversos meios podem ser empregados, como:

- Entrevista com as pessoas envolvidas;
- Análise de registros de e-mail;
- Auditoria de sistemas;
- Análise de imagens de vídeo.

Além do Comitê de Privacidade, o(a) Encarregado de Dados pode solicitar apoio de outras pessoas e áreas de dentro e fora da FEC, quando necessário.

Criticidade de um incidente

Baixa

São considerados incidentes de baixa criticidade os casos em que, por desvio de procedimento, dados pessoais possam ter sido:

- tratados por outros setores da FEC, que não os devidos;
- enviados a pessoas que já o possuíam, sem que se configure acesso não autorizado;
- enviados, sem condição de identificação do titular.

Alguns exemplos podem ser o envio acidental de dados de um bolsista para o coordenador do projeto, o envio de dados de um aluno para a secretaria do curso.

Média

Incidentes de média criticidade envolvem o tratamento indevido de dados pessoais identificáveis, mas sem grandes consequências gerais, tais como:

- Envio de dados de um titular a uma empresa sem autorização deste;
- Compartilhamento, com uma entidade ou pessoa, de arquivos com dados identificáveis quando deveriam ter sido ocultados;

Nesses casos o titular dos dados deve ser comunicado, com o fim de participar do processo de análise do incidente, inclusive identificando e mitigando possíveis riscos.

Alta

Casos de alta criticidade são eventos que envolvem vazamento de dados:

- Sensíveis;
- De grande volume de titulares;
- Incidentes de segurança cibernética, como ataques e invasões.

Nesses casos, tanto os titulares quanto a ANPD devem ser notificados o quanto antes, além de ser avaliada a necessidade de formalização de denúncias em âmbito civil e criminal.

3. Resposta

Realizada a análise do incidente, é necessário elaborar as ações de **Resposta ao Incidente**.

A Resposta ao incidente deverá variar em forma e abrangência com base nas determinações de criticidade e necessidades de comunicação ou não ao titular e autoridades, estabelecidas nas fases anteriores.

Em nenhum caso, por menor que seja a criticidade, **deve-se abandonar completamente a comunicação por escrito**, pois isto impede que os registros sejam posteriormente analisados e que se possa continuamente aprender com os eventos anteriores.

Em casos considerados de baixa criticidade, apenas comunicações por e-mail e verbais diretamente aos envolvidos podem ser suficientes, desde que não haja recorrência de eventos de incidente com as mesmas pessoas nem vazamento de dados. Casos em que haja recorrência podem demonstrar necessidade de informações mais aprofundadas, treinamentos e conscientização de pessoas ou grupos, por isso se recomenda comunicações por outras formas além das já mencionadas.

Em casos de média criticidade já se exige comunicação formal por e-mail ou ofício aos envolvidos, informando os eventos e as ações adotadas pela FEC para a solução ou mitigação do incidente, bem como para evitar que novos incidentes ocorram.

Nos casos mais graves, de alta criticidade, a LGPD determina a formalização de Comunicação de Incidente de Segurança, que deve ser realizada pelo(a) Encarregado(a) de Dados por meio de peticionamento eletrônico no site da ANPD.

Em todos os casos, recomenda-se que minimamente sejam comunicadas as seguintes informações:

- descrição geral do incidente e a data da ocorrência;
- natureza dos dados pessoais afetados e os riscos relacionados ao incidente;
- medidas tomadas e recomendadas para mitigar os efeitos do incidente;
- contato do encarregado ou o ponto de contato para que os envolvidos obtenham informações a respeito do incidente;
- outras informações que possam auxiliar a prevenir possíveis danos ou novos incidentes.

A decisão sobre a inclusão de destinatários na comunicação de um incidente deve dar-se na análise e considerar que todos os que tenham participado diretamente, além dos que possam aprender com o evento, podem ser comunicados, mas **não se deve de modo algum expor as pessoas, em especial os titulares de dados.**

Em todos os casos, recomenda-se refletir sobre que ações gerais de conscientização, informações complementares, treinamentos e demais instrumentos pedagógicos podem ser inseridos ou aprimorados, visando evitar novos incidentes. Note-se que aqui se trata de utilizar a ocorrência de um incidente como ponto de partida para novas ações, mas estas ações nunca devem utilizar os dados específicos e concretos de um incidente em particular, sob risco de expor pessoas desnecessariamente.

Além disso, em todos os casos alguma comunicação à Alta Gestão da FEC deve ser feita, de acordo com a criticidade:

- Baixa: apenas por e-mail com o relato geral do incidente e ações adotadas, ao fim do processo;
- Média: No momento da ciência do incidente, ao fim de cada fase do tratamento, informando o andamento e solicitando apoio quando necessário;
- Alta: No momento da ciência da criticidade do incidente, solicitando apoio para as tomadas de decisão e informando os avanços do tratamento. Nestes casos, pode-se decidir por instaurar um gabinete de crise para lidar com o incidente.

4. Registro

Todos os incidentes, independentemente da criticidade, devem ser registrados em meio eletrônico, seguro, próprio para o registro e sigiloso, contendo todas as informações e documentos reunidos no tratamento, bem como as respostas dadas.

Neste momento, o sistema de registro de incidentes da FEC é o Redmine, acessível aqui apenas aos membros do Comitê de Privacidade.

Como prevenir incidentes

A mais importante orientação a fazer em relação à proteção de dados e à gestão de incidentes é:

Prevenir incidentes é a melhor forma de gestão.

As ações voltadas à prevenção são sempre mais simples e menos custosas do que aquelas destinadas ao tratamento de um incidente ocorrido. Para compreender isto, basta refletir sobre que, em geral, apenas a atenção devida aos procedimentos já estabelecidos já é suficiente para a prevenção, enquanto qualquer incidente que ocorra, por menor que seja a sua gravidade, demandará os 4 processos de Identificação, Análise, Resposta e Registro, já mencionados anteriormente.

Assim, listamos a seguir uma série de orientações para auxiliar na prevenção de incidentes:

- Procure compreender o que são dados pessoais e com quais tipos de dados você já lida no seu cotidiano de trabalho;
- Ao receber informações pessoais, sempre verifique se a origem (quem lhe enviou) é a correta e se somente você e quem deveria, receberam.
- Durante suas atividades, certifique-se de manipular os dados pessoais apenas o mínimo necessário e de colocá-los nos locais corretos, sejam sistemas, arquivos na rede, envio por e-mail ou qualquer outra forma de utilização;
- Redobre a atenção ao encaminhar e responder e-mails que contenham dados pessoais, pois é comum que os destinatários se acumulem e, eventualmente, pessoas indevidas acabem por receber as informações.
- Ao enviar informações pessoais para outros setores e pessoas da FEC ou fora dela, verifique que apenas os destinatários corretos irão receber. Enviar por engano dados pessoais a pessoas indevidas fora da FEC é um vazamento de dados e pode ter consequências sérias.

Referências

- Lei Geral de Proteção de Dados,nº 13.709 de 14/8/2018
- Plano de Gestão de Incidentes com Dados Pessoais, do Ministério da Economia
- Comunicação de Incidente de Segurança à ANPD
- Guia de Resposta a Incidentes de Segurança, do Ministério da Gestão e Inovação
- Redmine FEC - Registro interno de incidentes


fec
Fundação
Euclides
da Cunha