POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EXTERNA

DATA DA ÚLTIMA ATUALIZAÇÃO: 07/12/2022.

Na FLASH, especificamos e criamos nossos produtos sobre uma base segura, com as proteções necessárias para manter a segurança dos usuários, dos dados e das informações que fazem parte das nossas atividades comerciais.

1. OBJETIVO

A Política de Segurança da Informação Externa tem como objetivo o cumprimento da transparência em relação aos clientes sobre as atividades relacionadas à Segurança da Informação executadas pela FLASH, bem como orientar aos fornecedores quanto ao mínimo de Segurança da Informação requerido deles no tratamento das informações referentes à FLASH.

2. REGRAS E NORMATIVAS APLICÁVEIS À PRESENTE POLÍTICA DA FLASH

- Lei n.13.709/2018 (Lei Geral de Proteção de Dados Pessoais);
- Lei n 12.965/2014 (Marco Civil da Internet);
- Resolução CMN nº 4.893, de 26 de fevereiro de 2021;
- Resolução do Banco Central nº 85, de abril de 2022;
- Normas e procedimentos internos que são constantemente revisados e aprovados pelas alçadas competentes e disponibilizadas a todos os colaboradores.

3. POLÍTICA PARA USO DOS ATIVOS

A criação de material impresso exibindo dados pessoais da FLASH deve ser evitada e, quando necessária, restrita e previamente consentida pela FLASH.

Quando materiais impressos forem destruídos, eles devem ser destruídos de forma segura, utilizando mecanismos como corte transversal, trituração, incineração ou desfibramento, por exemplo.

4. POLÍTICA PARA TRANSFERÊNCIA DE INFORMAÇÕES

Os dados pessoais transmitidos por redes públicas de transmissão de dados devem ser criptografados antes da transmissão.

Os dados pessoais transmitidos utilizando uma rede de transmissão de dados devem estar sujeitos a controles apropriados, projetados para assegurar que os dados alcancem o seu destino pretendido.

5. POLÍTICA DE CONTROLE DE ACESSO

Os colaboradores sob controle do fornecedor com acesso aos dados da FLASH, incluindo qualquer terceiro contratado pelo mesmo, devem estar sujeitos a uma obrigação de confidencialidade.

Devem existir procedimentos para registro e cancelamento do usuário que tratem a situação quando o controle de acesso do usuário estiver comprometido, como a corrupção ou o comprometimento de senhas ou outros dados de registro do usuário (por exemplo, como resultado de uma divulgação involuntária).

Deve existir um registro atualizado dos usuários ou perfis de usuários que tenham acesso autorizado ao sistema de informações.

Os dados pessoais armazenados no fornecedor ou fora de suas dependências devem estar sujeitos a um procedimento de autorização e não devem ser acessíveis a qualquer pessoa que não seja o pessoal autorizado. Que este conteúdo, por exemplo, esteja criptografado.

6. POLÍTICA DE BACKUP

Todo fornecedor contratado pela FLASH deve possuir a devida proteção de dados, assegurar a continuidade das operações assim como possibilitar a restauração após um sinistro.

O registro dos esforços de restauração de dados deve conter no mínimo: a pessoa responsável, uma descrição dos dados restaurados e os dados que foram restaurados manualmente.

A FLASH deve estar ciente do local onde essas cópias de segurança são mantidas pelo fornecedor, o tempo de retenção bem como cada fornecedor permite a exclusão dessas informações retidas.

7. POLÍTICA DE GESTÃO DE EVENTO

O fornecedor contratado pela FLASH deve deixar claro os critérios sobre se, quando e como as informações de registros podem ser disponibilizadas ou utilizadas, além de informar como garante a proteção desses registros para evitar a visibilidade dessas informações por pessoas não autorizadas, bem como inibir a exclusão desses registros antes do tempo.

O fornecedor deve determinar um tempo de retenção dos registros de eventos (logs) para garantir que a informação é devidamente apagada depois de um certo tempo.

8. POLÍTICA DE GESTÃO DE INCIDENTES

O fornecedor deve cooperar com a FLASH em todo incidente de segurança da informação, como por exemplo para determinar se ocorreu uma violação de dados que envolva dados pessoais e/ ou dados pessoais sensíveis..

Todo incidente de segurança da informação deve provocar uma análise crítica pelo fornecedor como parte de seu processo de gestão de incidentes de segurança da informação, para determinar se ocorreu uma violação de dados que envolvam dados pessoais.

9. POLÍTICA DE CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS

Deve-se ter certeza que os dados, incluindo todas as suas cópias e backups, estejam armazenados somente em localizações geográficas permitidas por contrato, SLA e/ou regulação.

Os fornecedores devem permitir que a FLASH monitore o desempenho do(s) serviço(s) contratado(s).

10. POLÍTICA DE ANÁLISE CRÍTICA DA SEGURANÇA DA INFORMAÇÃO

Todo fornecedor contratado pela FLASH deve comprovar que a segurança da informação é implementada e operada de acordo com as principais normas de segurança da informação, garantindo o mínimo exigido neste contrato.

O fornecedor deve permitir, quando solicitado, que a FLASH realize auditorias de Segurança da Informação.

Nos casos onde auditorias individuais pela FLASH forem impraticáveis ou possam aumentar os riscos à segurança, convém que o fornecedor disponibilize, antes da assinatura e durante um contrato, evidência independente de que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos do mesmo.

11. POLÍTICA PARA PROTEÇÃO DE INFORMAÇÃO PESSOAL

Consentimento e Escolha

Que o fornecedor forneça à FLASH os meios para capacitá-la a atender à sua obrigação de facilitar o exercício dos direitos dos titulares de dados pessoais a acessar, corrigir e/ou apagar seus respectivos dados.

Legitimidade e Especificação da Finalidade

Os dados pessoais tratados sob um contrato não devem ser utilizados para qualquer finalidade independente das instruções da FLASH.

Os dados pessoais não devem ser utilizados para fins de marketing e publicidade pelo fornecedor sem o consentimento expresso. Convém que este consentimento não seja uma condição de recebimento do serviço.

Limitação da Coleta

Não devem ser coletados dados pessoais indiscriminadamente. Tanto a quantidade quanto o tipo de dados pessoais coletados devem estar limitados ao necessário para cumprir o(s) objetivo(s) especificado(s) pela FLASH.

Minimização

Os arquivos e documentos temporários devem ser apagados ou destruídos dentro de um período especificado e documentado.

Limitação de Uso, Retenção e Divulgação

O fornecedor deve notificar a FLASH, de acordo com qualquer procedimento e períodos de tempo acordados no contrato, de qualquer solicitação legalmente vinculativa para divulgação dos dados pessoais por uma autoridade competente para cumprimento da lei, a menos que esta divulgação seja proibida.

As divulgações dos dados pessoais a terceiros devem ser registradas, incluindo qual dado pessoal foi divulgado, a quem e em qual momento.

Precisão e Qualidade

O fornecedor deve possibilitar meios para a FLASH assegurar aos titulares dos dados pessoais:

- tratamento preciso, completo, atualizado, adequado e pertinente para o objetivo de uso;
- a confiabilidade dos dados pessoais recolhidos a partir de uma fonte que não seja o titular de dados pessoais antes de ser tratado;
- por meios apropriados, a validade e a exatidão das reivindicações feitas pelo titular de dados pessoais antes de fazer qualquer alteração nos dados pessoais (a fim de assegurar que as alterações sejam devidamente autorizadas), quando for apropriado fazê-lo;
- procedimentos de coleta de dados pessoais para ajudar a garantir a precisão e a qualidade;
- mecanismos de controle para verificar periodicamente a precisão e a qualidade dos dados pessoais coletados e armazenados.

Abertura, Transparência e Notificação

O uso de subcontratados pelo fornecedor para tratar os dados pessoais deve ser divulgado à FLASH antes da sua utilização. Que também seja informado, em tempo hábil, sobre quaisquer alterações

pretendidas a este respeito, de modo que a FLASH tenha a capacidade de contestar estas alterações ou encerrar o contrato.

Os contratos entre o fornecedor e quaisquer subcontratados que tratam dados pessoais devem especificar as medidas técnicas e organizacionais mínimas que atendam à segurança da informação e às obrigações de proteção dos dados pessoais do fornecedor. Que estas medidas não sejam sujeitas à redução unilateral pelo subcontratado.

Que as informações divulgadas também incluam os países em que os subcontratados podem tratar os dados pessoais e os meios pelos quais os subcontratados são obrigados a atender ou exceder às obrigações do fornecedor.

Acesso e Participação Individual

O fornecedor deve possibilitar meios para a FLASH permitir aos titulares de dados pessoais:

- a capacidade de acessar e analisar criticamente os seus dados pessoais, desde que a sua identidade seja primeiramente autenticada com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;
- questionar a exatidão e a integridade dos dados pessoais e que sejam aperfeiçoados, corrigidos ou removidos conforme apropriado e possível no contexto específico;
- fornecer qualquer emenda, correção ou remoção sempre que solicitados;
- exercer seus respectivos direitos de forma simples, rápida e eficiente, o que não implica atrasos ou custos indevidos.

Responsabilização

Que os colaboradores sob controle do fornecedor com acesso aos dados pessoais da FLASH estejam sujeitos a uma obrigação de confidencialidade.

Os dados pessoais armazenados no fornecedor ou fora de suas dependências devem estar sujeitos a um procedimento de autorização e não devem ser acessíveis a qualquer pessoa que não seja o pessoal autorizado. Que este conteúdo, por exemplo, esteja criptografado.

Que o fornecedor atribua um ponto de contato para uso da FLASH referente ao tratamento de dados pessoais.

O fornecedor deve notificar prontamente a FLASH no caso de qualquer acesso não autorizado aos dados pessoais ou acesso não autorizado aos equipamentos ou instalações que resultem em risco de perda, divulgação ou alteração dos dados pessoais.

No caso de ocorrência de uma violação de dados que envolva dados pessoais, convém que um registro seja mantido com uma descrição do incidente, o período de tempo, as consequências do incidente, o nome da pessoa que reportou o incidente, a quem o incidente foi reportado, as medidas

tomadas para resolver o incidente (incluindo a pessoa responsável e os dados recuperados) e o fato de que o incidente resultou em perda, divulgação ou alteração dos dados pessoais.

Também, que um registro inclua uma descrição dos dados comprometidos, se forem conhecidos; e se notificações foram realizadas, as medidas tomadas para notificar a FLASH e/ou as agências reguladoras.

Para fins de descarte ou reuso seguro, os equipamentos que contêm mídia de armazenamento que possivelmente possam conter dados pessoais devem ser tratados como tal.

O fornecedor deve disponibilizar as informações necessárias para assegurar a FLASH que os dados pessoais tratados sob um contrato sejam apagados (pelo fornecedor e por qualquer um dos seus subcontratados) de onde quer que estejam armazenados, inclusive para fins de cópia de segurança (backup) e continuidade do negócio, assim que não sejam mais necessários para as finalidades específicas da FLASH ou após alcançar o período obrigatório de retenção para cumprimento de obrigações legais, regulatórias e/ ou fiscais.

Os dados pessoais devem ser destruídos de forma segura (desvinculação, sobregravação, desmagnetização, destruição ou outras formas de apagamento), inviabilizando a restauração de qualquer possível informação contida neles.

Transferência e Compartilhamento

O fornecedor deve especificar e documentar os países em que, possivelmente, os dados pessoais podem ser armazenados.

Que as identidades dos países decorrentes do uso de fornecedores subcontratados sejam incluídos. Quando acordos contratuais específicos se aplicarem à transferência internacional de dados, como Cláusulas de Contrato-Modelo, Regras Corporativas Vinculativas ou Regras de Privacidade Internacionais, convém que os acordos e os países ou circunstâncias em que estes acordos se aplicam também sejam identificados.

O fornecedor deve informar, em tempo hábil, ou sem demora indevida, à FLASH sobre quaisquer alterações pretendidas a este respeito, de modo que a FLASH tenha a capacidade de contestar estas alterações ou encerrar o contrato.

Avaliação de Fornecedores

Provedores e fornecedores que armazenam e processam dados, contratados pela FLASH, são avaliados sob o ponto de vista do nosso time interno de Segurança da Informação e devem seguir seus papéis e responsabilidades.

12. MUDANÇAS NA POLÍTICA

Esta Política de Segurança da Informação e Proteção de Dados pode passar por atualizações para refletir as melhorias realizadas. Desta forma, recomendamos a visita periódica desta página para que você tenha conhecimento sobre as modificações efetivadas.

Histórico de versões: Versão 1 de 07/12/2022.