LGPD
brasil.com.br

GUIA DE SEGURANÇA DA INFORMAÇÃO

PARA AGENTES DE PEQUENO PORTE

INTRODUÇÃO

Considerando a competência da ANPD, houve, a partir do art. 55-J, XVIII da LGPD, a edição de normas, orientações e procedimentos para micro empresas e empresas de pequeno porte. A partir da resolução em questão, foram incluídas no conceito de agentes de pequeno porte os Agente de Tratamento.Em virtude disso, fora criado o Guia de boas práticas, voltados para os agentes de tratamento de pequenos porte, apresentando algumas medidas de segurança da informação, de forma que haja o respeito e cumprimento aos arts. 46 a 49 da LGPD.

O conteúdo do resumo foi elaborado com base no Guia e nas disposições referidas da Lei Geral de Proteção de Dados (LGPD). O conteúdo original do **Guia pode ser acessado por meio do link:** *https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link- nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.*

1)GUIA DE SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE – BREVE RESUMO

Considerando a competência da ANPD, houve, a partir do art. 55-J, XVIII da LGPD, a edição de normas, orientações e procedimentos para microempresas e empresas de pequeno porte. A partir da resolução em questão, foram incluídas no conceito de agentes de pequeno porte os Agente de Tratamento.Em virtude disso, fora criado o Guia de boas práticas, voltados para os agentes de tratamento de pequenos porte, apresentando algumas medidas de segurança da informação, de forma que haja o respeito e cumprimento aos arts. 46 a 49 da LGPD.

2) COM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS, É PRECISO ESCLARECER ALGUNS PONTOS:

2.a) Segurança da Informação: Conjunto de ações que visam a preservação de confidencialidade, integridade e disponibilidade da informação. São importantes pois tais ações impactam o ambiente institucional de uma empresa, com o objetivo de prevenir, detectar e combater ameaças digitais. Um ponto importante é o Gerenciamento de Riscos no âmbito da segurança da informação visa identificar, quantificar e gerenciar os riscos. Embora não seja obrigatório, é fundamental pois integra as práticas de gerenciamento e das políticas de boa governança, bem como ajuda a melhorar a organização, desempenho e tomadas de decisões em empresas. Por tal razão, é recomendado que o gerenciamento de riscos de segurança seja realizado periodicamente.

2.b) Tratamento de Dados Pessoais: São todas as operações realizadas com dados pessoais, como as que envolvem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, com base no art. 5º, X da LGPD. Importante destacar que há dois conceitos presentes no art. 5º da LGPD. Em seu inciso I, os dados pessoais e, no inciso II, os dados sensíveis. Os dados sensíveis possuem regras mais rigorosas para seu tratamento pois possuem proteção especial pela LGPD, razão pela qual o rol de bases legais é distinto dos dados pessoais.

2.c) Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais: De acordo com o Princípio da Segurança (art. 6º, VII da LGPD) e com as normas presentes nos arts. 46 a 49, os agentes devem adotar medidas de segurança , técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, ou seja, vulnerabilidades que podem expor os dados dos titulares a tratamento inadequado ou ilícito. Tais medidas devem observadas desde a fase de concepção do produto ou do serviço até a sua execução (art. 46 caput e §2). Também devem ser garantidas a segurança da informação mesmo após o término do tratamento pelos agentes de tratamento (art. 47) . Além disso, caso haja possibilidade de risco ou dano relevante, a ANPD deverá ser comunicada (art. 48). Por fim, o art. 49 estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e nas demais normas regulamentares

2.d) Segurança da Informação relacionada a dados pessoais nos agentes de Tratamento de Pequeno Porte: Possuem relação com os já mencionados arts. 46, 47 e 49, bem como o art. 50 da LGPD, sendo baseadas em boas práticas internacionais. Porém, a implementação e manutenção de medidas podem necessitar de elevado investimento, impactando financeiramente os agentes de pequeno porte. Por tal razão, o guia apresenta sugestões para promover um ambiente institucional mais seguro quanto ao tratamento de dados pessoais.

3) MEDIDAS DE SEGURANÇA DA INFORMAÇÃO:

3.1.1) Medidas Administrativas – Política de Segurança da Informação (PSI) Consiste em um conjunto de diretrizes e regras para possibilitar o planejamento, implementação e o controle de ações relacionadas a segurança da informação. Ela pode ser endereçada por organizações de pequeno porte, representando uma boa pratica para a gestão de segurança. São incentivadas pela ANPD por evidenciar boa-fé e diligência na segurança de dados pessoais, além de fornecerem diretrizes na gestão de segurança da informação. A PSI possui o propósito de ser uma ferramenta que apoie a implementação de um processo estruturado de segurança da informação adequado a cada organização, considerando seu negócio e seu porte. Por tal razão, a ANPD recomenda:
Estabelecer uma política de segurança da informação simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como cópias de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de softwares, uso de correio eletrônico e uso de antivírus. Realizar revisões periódicas da política de segurança da informação. Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais

3.1.2) Medidas Administrativas - Conscientização e Treinamento

O sucesso das medidas que se referem à segurança da informação e à proteção de dados pessoais também estão atreladas com os recursos humanos de uma organização.Por tais razões, é importante realizar a conscientização dos funcionários, principalmente os envolvidos no tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD. Isso pode se dar via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD.

Além disso, é informar os funcionários sobre: como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail; manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas; não compartilhar logins e senhas de acesso das estações de trabalho; bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros; seguir as orientações da política de segurança da informação.

Também vale destacar ser importante criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas.

3.1.3) Medidas Administrativas - Gerenciamento de Contratos:

Assinar termos de confidencialidade (non-disclosure agreement - NDA) com os funcionários da empresa acaba sendo recomendável, para que se comprometam a não divulgar informações confidenciais que envolvam dados pessoais. Uma medida importante contra abuso de privilégio.

No caso de agentes de tratamento de pequeno porte que terceirizam os serviços de TI, é recomendado estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como: regras para fornecedores e parceiros; regras sobre compartilhamentos; relações entre controlador-operador; orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

3.2.1) Medidas Técnicas - Controle de Acesso: É fundamental, como medida técnica, implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais. Consiste em processos de autenticação (identificação de quem acessou), autorização (o que podem fazer) e auditoria (o que foi feito). A ANPD, por conta disso, recomenda ao agente de pequeno porte a Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade. **Além disso, também recomenda a implementar um adequado gerenciamento de senhas, estabelecendo controles tais como:** Evitar o uso de senhas padrão (default) disponibilizadas pelos fornecedores de software ou hardware adquiridos; utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos; não reutilizar senhas.
Deve ser aplicado o princípio do menor privilégio (need to know) de forma a proibir o compartilhamento de contas ou de senhas entre funcionários. É recomendado também utilizar a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais para aumentar a segurança da informação.

3.2.2) Medidas Técnicas - Segurança dos Dados Pessoais Armazenados: Até o momento, todas as etapas descritas visam contribuir para a segurança dos dados pessoais armazenados, a fim de diminuir o risco de incidentes e aumentar a segurança que os agentes de pequeno porte devem ter ao longo do tratamento de dados pessoais. Por isso, como uma boa medida de segurança é importante coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados, considerando o art. 6º, III da LGPD que versa sobre o principio da necessidade.

É recomendado também a implementação de soluções de pseudonimização, como a criptografia, para cifrar dados pessoais sensíveis, para dificultar a identificação do titular de dados.
Dentre outras medidas, fundamental é orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho; Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos (considerando o risco de se perder a guarda dos dados pessoais transferidos.) e, caso tal operação seja imprescindível, inventariar e cifrar dados de dispositivos externos e armazena-los em locais seguros .
Realizar backups offline, periódicos e armazená-los de forma segura. Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas. Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte).

3.2.3) Medidas Técnicas - Segurança das Comunicações: Possuem relação exatamente com um importante ponto relacionado a segurança de dados, diante da possibilidade de vulnerabilidades na transmissão de dados ou informações (Links maliciosos, por exemplo).
Destaca-se, dentre boas medidas de segurança, utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim-a-fim para serviços de comunicação; Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF – Filtro de Aplicação) para detectar e bloquear ameaças e impedir conexões a redes não confiáveis; Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e, integrar o antivírus ao sistema de e-mail.
Por fim, é recomendado Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas, como o site da empresa. Caso o negócio da empresa envolva tal tratamento com dados sensíveis, é recomendado criar um canal de acesso restrito para o cliente acessar tais informações.

3.2.4) Medidas Técnicas - Gerenciamento de Vulnerabilidades:
Importante ponto relacionado com o monitoramento da existência de novas versões e correções disponíveis em todos os sistemas e aplicativos. Sendo assim, é recomendado atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os funcionando, ativamente (de forma que não possam ser desativados ou alterados pelos usuários) em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores). Por fim, é recomendado aos agentes de tratamento a adotar e atualizar periodicamente softwares antivírus e antimalwares e realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

3.3 - MEDIDAS RELACIONADAS AO USO DE DISPOSITIVOS MÓVEIS:

Com relação a tais dispositivos, a recomendação é que os mesmos procedimentos de controle de acesso a equipamentos de TI sejam utilizados como técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops (guardados em locais seguros quando não estiverem em uso) e sistemas de informação.
Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível, também é importante, considerando a vulnerabilidade que dispositivos de uso privado possam trazer pelo uso de aplicativos potencialmente inseguros para fins pessoais, não havendo o gerenciamento no acesso e nos aplicativos como ocorre com os dispositivos institucionais.
Por fim, diante da possibilidade de perda ou roubo dos dispositivos, importante implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

3.4 – Medidas relacionadas aos Serviços em Nuvem: Como medidas prioritárias para garantir uma maior garantia na proteção de Dados Pessoais na contratação de serviços em nuvem, é importante realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados. Também é importante Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos, bem como Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado e Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais.

CONSIDERAÇÕES FINAIS:

O presente guia visa exatamente a simplificar a compreensão com relação aos deveres, responsabilidades, bem como com relação as boas práticas e medidas básicas de segurança para apoiar os a agentes de tratamento de pequeno porte no desenvolvimento de suas atividades

Vale lembrar que o guia em questão não possui efeito normativo vinculante, devendo ser entendido apenas como um guia de boas praticas

O intuito do guia era de contribuir para um ambiente mais saudável e seguro com relação ao tratamento de dados pessoais e, também, para um ambiente onde a confiabilidade nos negócios seja cada vez maior

LGPD
brasil.com.br

MATERIAL PRODUZIDO POR

Mateus Reis dos Santos Alves