CARTILHA COM DIRETRIZES SOBRE A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Sumário

APRESENTAÇÃO

Essa cartilha é fruto de um trabalho coletivo dos membros da Comissão Permanente de Direito Digital e de Proteção de Dados Pessoais (LGPD) da Divisão Jurídica da FEDERASUL, que tem como objetivo oferecer aos associados e ao público em geral um material contendo diretrizes básicas a respeito do processo de adequação das empresas à Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/18) e do seu permanente cumprimento.

O processo de adequação não é um passo simples, nem rápido, mas uma verdadeira jornada, já que envolve a revisão de práticas até então consolidadas com os consumidores, com os parceiros de negócios e com os empregados e colaboradores. Envolve, também, uma nova forma de fazer negócio e de se relacionar com o mercado.

A LGPD, como o nome bem diz, é uma lei geral, aplicável a todas as empresas e segmentos da economia. Sua finalidade principal é preservar o direito das pessoas físicas, titulares dos dados, quanto à determinação e o controle dos usos que serão conferidos aos seus dados pessoais. E para assegurar os direitos dos titulares exige, por outro lado, que as empresas estejam aptas a fazer frente a tais direitos.

Sob a dimensão das empresas, portanto, fica o desafio de rever o modo de operar no mercado, tomando em consideração a privacidade do titular dos dados, desde a fase de planejamento dos serviços e produtos a serem ofertados. Importante ter em mente que o propósito da LGPD não é barrar o avanço tecnológico ou a inovação, mas, sim, fomentá-los conjugando o desenvolvimento econômico à proteção dos dados pessoais e a preservação da privacidade.

Este material não tem o propósito de ser exaustivo, tampouco dispensa uma assessoria especializada, tanto jurídica quanto de segurança da informação, para a condução do processo de adequação.

Esperamos, por meio deste material, poder contribuir para esclarecer a importância e a necessidade da adequação a LGPD, bem como para prover uma visão geral do passo a passo a ser dado em direção a tal conformidade.

Fernanda Girardi Tavares

Membro e Coordenadora da Comissão Permanente de Direito Digital e de Proteção de Dados Pessoais (LGPD) da Divisão Jurídica da FEDERASUL (gestão 2020/2022)

NOTA A 2ª EDIÇÃO

O lançamento da segunda edição desta cartilha é realizado em janeiro de 2024. O cenário atual, decorridos pouco mais de 5 anos da sanção da Lei Geral LGPD, é bem diferente daquele que nos encontrávamos quando do lançamento da primeira edição, no ano de 2020.

A implementação da LGPD não foi, e mesmo em 2024 continua não sendo, isenta de obstáculos. A transição para um ambiente de conformidade com a lei apresentou uma série de desafios para empresas. Entre os desafios iniciais na implementação estava a estruturação de mecanismos técnicos e organizacionais que possam garantir o respeito à legalidade no tratamento de dados pessoais, aliados a boas práticas corporativas, através de programas de compliance e governança.

Ademais, tornou-se indispensável a elaboração de um mapeamento de dados pessoais e, tarefa nem de perto é fácil, sendo necessária a participação e o engajamento dos diversos departamentos para o sucesso do mapeamento. A partir do mapeamento revelam-se os riscos a serem mitigados, o plano de mitigação e a construção da política de conformidade da organização, que deve estar de acordo com a estrutura e com o escopo da operação envolvendo o tratamento de dados pessoais.

Outras providências tornaram-se igualmente importantes, tais como a adequação de documentos e processos, incluindo termos de uso e de políticas de privacidade para clientes e colaboradores; a revisão de contratos e processos com subcontratados, fornecedores, parceiros e outros terceiros; definição de políticas e processos internos; a construção de estrutura de obtenção de consentimento dos clientes, conforme o uso e a destinação dos dados; a construção de regras e rotinas para atender às solicitações e reclamações dos titulares de dados; a adoção de medidas de segurança técnicas e administrativas para proteção dos dados.

No meio do caminho, a Autoridade Nacional de Proteção de Dados (ANPD), em atuação multifacetada, envolvendo a conscientização e orientação da sociedade sobre a LGPD, publicou guias orientativos sobre temas como segurança da informação, cookies e agentes de tratamentos de dados. Ainda, regulamentou o tratamento de dados para agentes de tratamento de pequeno porte, o processo de fiscalização e processo administrativo, além da dosimetria e sanções das multas. Esses materiais oficiais agora podem ser utilizados juntamente com esta nova versão da cartilha, para guiar os associados e o público em geral na jornada contínua de conformidade à LGPD.

Marcela Joelsons

Coordenadora da Comissão Permanente de Direito Digital e de Proteção de Dados Pessoais (LGPD) da Divisão Jurídica da FEDERASUL (gestão 2023)

I. INTRODUÇÃO: POR QUE SE ADEQUAR À LEI GERAL DE PROTEÇÃO DE DADOS?

A Lei n.º 13.709 foi publicada em 14 de agosto de 2018 e conhecida como Lei Geral de Proteção de Dados (LGPD) e está em vigor desde agosto de 2020, salvo quanto aos dispositivos que tratam das sanções administrativas, que vigoram desde agosto de 2021. Além disso, em 27 de fevereiro de 2023 foi publicado o Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela Autoridade Nacional de Proteção de Dados (ANPD), o que significa que, a partir disto, a ANPD possui todas as ferramentas para a efetiva fiscalização e imposição de penalidades, incluindo as multas. Nesse sentido, a ANPD, ao longo de 2023, tem realizado fiscalizações e já deu início à aplicação de penalidades, incluindo multa.

A norma se aplica a pessoas físicas e jurídicas de direito público e privado, que realizam o tratamento de dados, bem como às pessoas físicas que têm seus dados coletados, independentemente do meio (físico ou digital), do país de sua sede ou do país onde estejam localizados os dados. O tratamento de dados, por sua vez, de acordo com a LGPD, consiste em *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.*

Quaisquer informações que possam levar à identificação de uma pessoa, de maneira direta ou indireta, por referência a um nome, a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social, são considerados dados pessoais.

Assim, é imprescindível que as empresas adequem suas rotinas e procedimentos à nova norma e, efetivamente, considerem os impactos que a norma trará para o seu dia a dia, com relação ao objeto e à destinação do

negócio, bem como com relação aos dados de seus clientes, produtos, fornecedores, equipe de prestadores e empregados.

Em atenção ao regramento, a empresa tem a obrigação de designar a pessoa responsável pela proteção dos dados, o Encarregado da Proteção de Dados, ou DPO (*Data Protection Officer*). Este responsável é a pessoa indicada pelo Controlador para ser o elo entre o Controlador, os Titulares e a ANPD, bem como por disseminar a cultura de proteção de dados e orientar os empregados sobre práticas de tratamento de dados, entre outras.

De acordo com a Resolução CD/ANPD Nº 02 microempresas, empresas de pequeno porte e startups (exceto as que se enquadrem no artigo 3º da resolução) não necessitam designar um Encarregado, embora devam manter canal de comunicação disponível aos titulares de dados. Segundo a ANPD, "no entanto, é certo dizer que o porte de uma empresa não altera o direito fundamental que o titular de dados tem à proteção de seus dados pessoais, nem desobriga que as atividades de tratamentos de dados observem a boa-fé e os princípios da lei, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas".

Além disso, é recomendável que as empresas implantem uma política de governança ou programa para proteção de dados e coletadas autorizações/consentimentos específicos, quando for o caso, para o uso destes dados anteriormente armazenados, em conformidade com a nova lei. A implantação desta Política de Governança/Segurança para guarda e uso dos dados pessoais, com transparência e confiabilidade, é imprescindível.

O desenvolvimento da Política de Governança/Segurança da Informação e a catalogação destes dados hoje mantidos permitirá definir, entre outras questões: (a) quais são os dados que mantenho hoje armazenados? (b) quais são os dados que legalmente devo ou posso manter e qual a base legal para tanto? (c) quais são os dados imprescindíveis ao desenvolvimento da atividade social da empresa; (d) por quanto tempo preciso/sou autorizado a manter estes dados armazenados? (e) como proteger os dados armazenados? (f) quais são os dados

que disponho e poderão ser descartados? (g) quais são os dados que pretendo manter e dependem de autorização do titular para armazenamento e tratamento?

É igualmente necessário que sejam discutidas e implantadas políticas internas que desenvolvam essa matriz de identificação e catalogação, bem como que disponham sobre a forma de tratamento dos dados que serão mantidos (inclusive quanto à obtenção de autorização para manutenção e utilização destes dados quando for o caso), tudo a fim de comprovar que a empresa desenvolveu, efetivamente, esforços para obter as autorizações e proteger os dados de seus colaboradores e familiares.

A forma de guarda, tratamento e mesmo o monitoramento do uso destes dados (e sua rastreabilidade – ou seja, os caminhos que estes dados irão percorrer e quem os manuseará) deve estar descrita e bem representada na Política de Segurança da Informação que deverá ser desenvolvida.

Precisamos ter presente que este é um processo vivo, uma rotina com constante necessidade de revisão, divulgação e treinamentos, na medida em que, a cada nova obrigação de informação, fica reavivada a necessidade de adequação dos dados que serão guardados e a necessidade do novo treinamento ou retreinamento da equipe.

Não menos importante é considerar que as empresas precisam estar preparadas para, na forma que determina a LGPD, em caso de vazamento de dados que venha a resultar em algum risco ao titular, realizar a comunicação do incidente de segurança tanto ao titular quanto à ANPD, conforme orientações da autoridade que podem ser acessadas aqui. Esta disposição deverá compor a política de segurança a ser desenvolvida e ser objeto de comunicação, se porventura ocorrer o vazamento em questão.

Enfim, muitas frentes e oportunidades diferentes surgem a partir desta norma de proteção – a ensejar a aplicação das rotinas diárias de gestão, em consonância com a nova legislação – tudo na forma que será objeto dos capítulos seguintes desta cartilha.

II. ETAPAS DO PROCESSO DE ADEQUAÇÃO

Em linhas gerais, um projeto de implementação dos requisitos previstos na LGPD pode ser estruturado em 3 (três) grandes fases:

(i.) Mapeamento de dados;
(ii.) Avaliação de risco; e
(iii.) Plano de ação e implementação.

Sinteticamente, o **mapeamento** consiste no levantamento de todos os fluxos de dados da empresa, sendo que a **avaliação de risco** consiste na análise crítica de tal levantamento para que sejam identificadas as possíveis não conformidades do ponto de vista legal e técnico. Por fim, o **plano de ação** indicará todas as medidas concretas a serem adotadas para adequação e a fase de **implementação**, por sua vez, corresponderá à efetiva adoção de tais providências práticas.

A adequação à LGPD deverá levar em consideração o porte da empresa e seu perfil, considerando particularidades, tais como setor de mercado que atua, se é controlada por alguma agência reguladora e está sujeita a normas setoriais específicas, se atua somente em território nacional ou também no exterior, sua estrutura organizacional, quantidade de funcionários, parceiros, fornecedores, empresas coligadas, terceiros envolvidos.

II.1. Mapeamento de dados

Este tópico abordará a primeira etapa de implantação, em que é essencial um mapeamento 360º da empresa para que se possa identificar e avaliar as operações e fluxos de dados realizados pelas empresas.

A partir disso, para cumprirem e adequarem-se à LGPD, as organizações precisam conhecer o status e os contextos nos quais inserem-se os dados pessoais relacionados às pessoas físicas. Isso é possível por meio do

mapeamento de dados e seus fluxos, possibilitando uma melhor e mais precisa avaliação dos riscos à segurança e à privacidade.

Como parte integrante de um inventário e de auxílio a processos de *assessment* (processos de recrutamento, seleção, avaliação, etc) e tratamento de dados, intrinsecamente referendados nos artigos 37 e 38 da LGPD, temos o mapeamento de dados, ou *data mapping*. Trata-se de um levantamento detalhado que abrange, dentre outros, os tipos, condições, natureza, trilhas, relação entre os dados e bases de armazenamento dos dados coletados.

Nessa fase, verifica-se quais dados são coletados, o local onde estão armazenados os dados e respectivo formato, políticas de acesso, justificativa para a respectiva coleta, usos dos dados, tempo de armazenamento, identificação quanto à transferência ou compartilhamento dos dados.

Tal levantamento permite identificar e compreender o tratamento habitualmente realizado, bem como os riscos e vulnerabilidades, inclusive sob a perspectiva de segurança da informação, existentes.

O mapeamento de dados, portanto, tem a finalidade de catalogar dados obtidos e/ou coletados pelas organizações, a forma como são usados, onde são armazenados, qual o tráfego percorrido na organização e como e para quem são transferidos. Busca-se identificar, nesta etapa, quais são, efetivamente, os dados ***tratados*** e o ciclo de vida de tais dados.

Existem várias maneiras de obter o mapa de dados ou realizar o mapeamento, seja por meio de uma planilha simples ou de um programa ou sistema de mapeamento de dados integrado. A extensão, complexidade ou limite do mapeamento de dados dependerá da complexidade e extensão do negócio e suas cadeias produtivas.

A partir desse conceito, é importante que o mapa evidencie as seguintes informações sobre os dados pessoais:

(i.) Quais dados são coletados;
(ii.) Tipos, origem e destino dos dados;

(iii.) Características, natureza e criticidade (sensível ou não);

(iv.) Fundamento legal para o processamento de tais dados (incluindo referência expressa às bases legais que autorizam o tratamento de dados, previstas no artigo 7º da LGPD);

(v.) Finalidade da coleta de dados;

(vi.) Onde estão armazenados – se em meio digital ou analógico e demais dados de rastreabilidade;

(vii.) Privilégios de acesso;

(viii.) Duração e período de armazenamento;

(ix.) Condições de armazenamento (com a indicação das medidas protetivas disponibilizadas pela organização) e forma de tratamento, desde a coleta até a eliminação;

(x.) Ocorrência de transferência de dados;

(xi.) Localização dos destinatários de transferência dos dados (registro das transferências nacionais e internacionais); e

(xii.) Protocolos de proteção durante as transferências (em caso de transferências internacionais, se o País de destino tem regulação e autoridade (órgão) de privacidade).

Para a realização de um mapa de dados eficaz, é preciso que as unidades corporativas de negócios, especialmente os departamentos de TI, jurídico, marketing e RH, se envolvam em tal processo.

Esta primeira etapa da implementação é um elemento de extrema importância na adequação da organização às diretrizes da LGPD. A adequada avaliação de segurança e privacidade existentes demanda o rastreamento dos dados desde o ponto de coleta até sua exclusão – de modo que, sem uma visão geral de todo o ciclo de vida dos dados, quaisquer procedimentos de segurança, proteção e privacidade podem estar comprometidos.

Cabe, ainda, apontar que todo mapeamento de dados de organizações distintas terá as especificidades daquela determinada empresa e será diretamente proporcional.

Por fim, vale reiterar que não existe uma maneira única de realizar um processo de mapeamento de dados, devendo ser eleito o método mais condizente ao porte e à complexidade das operações da organização em questão.

II.2. Avaliação de risco

Realizado o mapeamento dos fluxos de dados, é necessário um olhar crítico para os processos de negócio da empresa que envolvam dados pessoais. Essa análise crítica é essencial para se poder verificar quais práticas não estão ainda em conformidade com a LGPD e geram, portanto, descumprimento e risco de exposição das empresas a sanções e a pleitos dos titulares ou de órgãos fiscalizatórios.

A mensuração de riscos, ou seja, o *risk assessment* deve identificar não apenas potenciais descumprimentos das obrigações estabelecidas LGPD, mas também o nível de criticidade e de exposição quanto a possíveis vazamentos de dados por processo de negócio. Tal facilita, consideravelmente, a elaboração de um plano de ação estruturado para mitigar cada um dos pontos levantados, como acompanharemos a seguir.

A empresa que vislumbra a melhor implementação e adequação das exigências previstas na LGPD deve trabalhar a gestão de riscos dos processos que fazem parte de suas estruturas, buscando identificar os impactos positivos e negativos de situações que possam acarretar algum prejuízo, não só para o negócio, mas, também, para a imagem da empresa.

Segundo o Guia PMBOK (2008)[1], o gerenciamento de riscos inclui processos de planejamento, identificação, análise, planejamento de respostas, monitoramento e controle de riscos de um projeto. O gerenciamento de riscos tem como objetivo

[1] Guia do Conhecimento em gerenciamento de projetos. Guia PMBOK. 4ª Edição. Disponível em: https://www.docsity.com/pt/pmbok-2008/4884280/. Acesso em: 22 de abril de 2020.

aumentar o impacto dos eventos positivos e reduzir o impacto dos eventos negativos.

Trata-se de uma análise sistemática de todos os aspectos relacionados ao tratamento de dados pessoais dentro da companhia e que identificará todos os processos vulneráveis suscetíveis à má utilização ou tratamento inadequado dos dados.

Este levantamento oportunizará, ainda, atuar de maneira direcionada e específica para prevenir de forma eficiente e eficaz a possibilidade de ocorrências de eventos indesejáveis e exposições da empresa sob o ponto de vista da LGPD.

Além disso, será possível estabelecer regras, políticas e manuais para monitoramento contínuo, promovendo a atualização e ajustes necessários conforme novos riscos forem se apresentando ao longo da governança de dados.

II.3. Plano de ação e implementação

Feito o mapeamento e o diagnóstico de riscos, passa-se à construção de um plano de ação e sua subsequente implementação prática. O plano de ação consistirá no planejamento prático das medidas concretas a serem adotadas pela empresa para eliminar ou mitigar os riscos detectados.

Portanto, o diagnóstico e a avaliação feitos nas etapas anteriores permitirá identificar e traçar as medidas – quer sejam de natureza jurídica ou técnica – que viabilizarão a conformidade da empresa com as diretrizes e obrigações previstas pela LGPD. Trata-se do exercício de analisar as práticas que, confrontadas com a LGPD, podem configurar descumprimentos e que, portanto, considerando o grau de risco, podem ser alteradas.

A partir disso, temos que o Plano de Ação abrange um delineamento das práticas internas que podem ou devem ser alteradas, revisão de políticas de privacidade,

termos de uso, contratos com terceiros, quer seja com empregados, prestadores de serviços, fornecedores, canais e demais parceiros comerciais ou clientes – tudo à luz da análise de riscos. Além disso, engloba, também, em um segundo momento, a implantação de mecanismos de segurança da informação para assegurar que as medidas preventivas de eventuais incidentes tenham sido adotadas.

Em síntese, pode ser indicado o seguinte grupo de medidas práticas exemplificativas:

(i.) adoção de ferramentas técnicas que permitam maior segurança e sejam aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

(ii.) revisão de documentos, abrangendo contratos e políticas;

(iii.) estabelecimento de uma governança digital e boas práticas;

(iv.) realinhamento do *mindset* / mudança cultural quanto ao tratamento de dados, com a internalização da diretriz de que a empresa deve limitar o tratamento de dados ao mínimo necessário para a realização de suas finalidades;

(v.) criação de processos internos voltados à eliminação de dados após o término do tratamento;

(vi.) estabelecimento de mecanismos internos de segurança dos dados e de detecção de eventuais incidentes (e.g. criptografia, anonimização);

(vii.) definição de um Encarregado (DPO), quando determinado por lei, que pode ser próprio ou terceirizado;

(viii.) manutenção de documentação atualizada com o registro das operações de tratamento dos dados, de modo a viabilizar a extração de Relatório de Impacto à proteção de dados pessoais;

(ix.) criação de política interna contemplando plano de respostas a incidentes de vazamento de dados e/ou de segurança;

(x.) criação de processo interno voltado ao atendimento dos direitos dos titulares, que podem requisitar a qualquer momento, por exemplo, a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a portabilidade dos dados a outro fornecedor de serviço ou produto quando for o caso, a eliminação dos dados pessoais tratados com o consentimento do titular, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, a revogação do consentimento.

Há ações específicas a serem adotadas com relação a temáticas e áreas específicas nas empresas, também em conformidade com as atividades desenvolvidas.

Cabe citar, a título ilustrativo e exemplificativo, providências aplicáveis à relação das empresas com os **clientes/consumidores**:

(i.) Contratos, Termos de Uso e Políticas de Privacidade: deve ser conferida atenção à forma e ao conteúdo, especialmente quanto à informação sobre as situações de tratamento de dados e sua respectiva base legal, bem como quanto à obtenção do consentimento para o tratamento de dados quando for o caso (nas situações em que houver necessidade de obtenção do consentimento);

(ii.) Revisão de processos internos, online e/ou offline (incluindo os serviços de atendimento ao cliente), que se relacionem ao tratamento de dados e ao atendimento dos direitos dos titulares.

Outro ponto que deve constar no plano de ação são as providências práticas nas **relações trabalhistas**:

(i.) Revisão do processo seletivo de profissionais;
(ii.) Revisão dos processos de admissão e desligamento para que seja preservada a privacidade dos titulares;

(iii.) Avaliação quanto à necessidade de que os empregados tenham que conferir consentimentos específicos para eventual tratamento de dados (para finalidade distinta da contratação propriamente ou do cumprimento de obrigações legais pela empresa) e eventual necessidade de modificação dos contratos de trabalho;

(iv.) Avaliação quanto às práticas de retenção de dados após o encerramento dos contratos de trabalho;

(v.) Avaliação quanto à gestão de dados pessoais sensíveis dos empregados.

Nas relações com os **prestadores de serviços** e **fornecedores** faz-se também necessário incluir no plano de ação medidas tendentes a:

(i.) Avaliação dos contratos e estipulação de cláusulas prevendo o cumprimento de requisitos de conformidade quanto à proteção de dados pessoais;

(ii.) Estabelecimento de padrões de serviços e requisitos técnicos de segurança, além de obrigações compatíveis com as exigências da LGPD: manutenção do registro dos tratamentos de dados efetuados, necessidade de comunicações a serem realizadas à Autoridade Nacional e aos titulares em caso de incidentes de segurança, exigência quanto à adoção de mecanismos de segurança, responsabilidade das partes e alocação de riscos.

Além disso, o plano de ação deve contemplar a realização de **treinamentos internos** para capacitar os gestores e colaboradores quanto ao tema de proteção de dados pessoais, as obrigações legais e políticas adotadas pela empresa.

Após a **implementação das medidas práticas**, mostra-se recomendável a emissão do relatório de implementação, contendo a descrição de todas as atividades tomadas e os passos seguintes para a manutenção da conformidade.

Subsequentemente, deve-se realizar o **monitoramento** da implantação das medidas de adequação para que seja possível aferir se estão de fato sendo seguidas pelos colaboradores e agentes envolvidos nos processos.

II.4. Treinamentos e ações educativas

A LGPD não apenas impõe obrigações legais às empresas, mas também enfatiza a responsabilidade compartilhada na proteção dos dados pessoais.

Treinamentos sobre este tema ajudam a evitar riscos legais e financeiros para as empresas. Além disso, demonstram o compromisso com a proteção de dados gerando assim, confiança dos clientes, parceiros, fornecedores, colaboradores.

Colaboradores capacitados e bem treinados são menos propensos a cometer erros que levem a violações de dados, auxiliando a evitar vazamentos de informações sensíveis e os problemas associados a eles.

Além disso, ações educativas sobre proteção de dados promovem a conscientização e a compreensão sobre LGPD em toda a organização, gerando uma cultura de respeito à privacidade.

É um investimento que não pode ser negligenciado em um ambiente onde a segurança e a confiança são fundamentais para adaptação às novas ameaças e desafios que surgem regularmente.

Tais ações podem ser feitas através de palestras, presenciais ou on-line, vídeos, podcasts, e até mesmo com a utilização de jogos interativos. Além disso, devem ser realizados periodicamente, para garantir a constante atualização e conscientização dos colaboradores da empresa.

São temas importantes a serem abordados:

- Noções gerais sobre a LGPD;
- Apresentação do encarregado e dos canais de comunicação existentes;
- Informações sobre as providencias adotadas pela empresa para o cumprimento da lei;
- Apresentação das Políticas de Privacidade e de Segurança da Informação.

- 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;
- Orientações sobre armazenamento de documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- Sigilo e troca periódica de logins e senhas de acesso das estações de trabalho;
- Bloqueio de computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- Necessidade de informar incidentes e vulnerabilidades detectadas.

Tão relevante quanto o treinamento em si é o registro dele, seja por meio de lista de presença, gravação ou declaração a ser assinada pelos participantes. Isso pode ajudar a evitar multas e outras penalidades aplicáveis às empresas que não estejam em conformidade com a LGPD.

III. BOAS PRÁTICAS

A primeira razão para se investir em boas práticas de governança relacionada à proteção de dados se refere à necessidade de que as normas constantes na LGPD sejam efetivadas nas empresas. Com a implementação de mecanismos que garantam a segurança nas atividades empresariais no tratamento de dados, se viabiliza a garantia dos direitos dos titulares dos dados e a confiança do mercado (consumidores) no serviço prestado pela empresa.

Outro benefício em investir em programas de adequação à LGPD, com a instituição das boas práticas, é a sua representação como fator de demonstração aos órgãos de investigação das tentativas da empresa para respeitar todas as determinações da Lei.

Embora a ANPD tenha, entre as suas atribuições, a função de promover a fiscalização dos agentes de tratamento de dados (e aplicar eventuais sanções administrativas), vale ter em mente que pode haver investigações também por outros órgãos, como o Ministério Público e PROCONS – no limite de suas respectivas competências.

Nesse sentido, a LGPD, em seu artigo 52, § 1º, IX, determina que, no caso de cometimento de infrações legais, sejam consideradas, na aplicação das respectivas sanções, as boas práticas e a governança instituídas pela empresa. Ainda, de acordo com o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, a adoção de boas práticas constitui circunstância atenuante na fixação de eventual multa pela ANPD. Assim, apesar de não ser uma forma de afastar punições, a implementação de boas práticas serve como forma de atenuar as sanções que possam vir a ser aplicadas pela ANDP.

Outro efeito relevante que decorre da adoção de um programa de governança de dados é a demonstração, não só frente a ANPD, mas também para o mercado, da idoneidade da empresa em relação às suas práticas de proteção de dados. Os consumidores, cientes da segurança dos seus dados com o tratamento feito pelas empresas, terão uma maior confiança no serviço prestado, aumentando a disposição para contratá-lo. Não há dúvida de que a

conformidade com a LGPD e a adoção de boas práticas consistirá em um diferencial competitivo no mercado.

De mais a mais, qualquer empresa em processo de implementação da LGPD deve ter em mente que o trabalho não se extingue com o término do processo formal de adequação. Trata-se de um processo em movimento, que começa com a implementação em si, mas que continua por meio da atividade diária da empresa, sendo imprescindíveis o seu acompanhamento e atualização.

É nesse ponto que as organizações têm se deparado com os maiores desafios: corrigir procedimentos inadequados aos olhos da LGPD e manter as boas práticas indicadas como solução. A dificuldade está justamente na manutenção a longo prazo, uma vez que não basta a adoção de determinada conduta por tempo específico.

As empresas precisam incutir a mudança em sua estrutura, inclusive culturalmente. E sabemos que mudar comportamentos envolve um trabalho complexo e de paciência, além de um contínuo cuidado e de revisão de processos.

O tratamento dos dados deve observar uma conduta proativa e jamais reativa, de forma a antecipar a ocorrência de quaisquer eventos que coloquem em risco a privacidade das informações dos clientes. A abordagem é de prevenção, e não de reação, medidas conhecidas como Privacidade desde a Concepção e por Padrão (*Privacy by Design / by Default)*.

Para funcionar – independentemente do tamanho da empresa – é essencial que o alto escalão da organização se comprometa com essas boas práticas, de forma a fazer cumprir todos os padrões e protocolos de privacidade.

Ambas as medidas prezam por garantir que a organização, por padrão, faça o tratamento apenas dos dados pessoais necessários para o cumprimento da finalidade para a qual tal dado foi coletado. Por isso é importante que a empresa saiba exatamente por qual razão precisa do dado pessoal em questão e por quanto tempo terá de armazená-lo.

Para atender à LGPD por meio da adoção de boas práticas de privacidade de dados, é importante que a empresa:

I. Revise as políticas de segurança das informações para alinhar procedimentos e corrigir possíveis problemas. Nesse momento, é interessante criar um programa de governança que disponha das normas e políticas internas sobre a proteção e tratamento de dados para que todos os colaboradores tenham acesso e saibam o posicionamento da corporação.

II. Fique atenta aos dispositivos que os colaboradores trazem de casa. Se a empresa permite o uso de dispositivos de armazenamento como *smartphones* e *pen drives*, por exemplo, é importante que todos os colaboradores conheçam as políticas de segurança de dados e que a empresa reforce a segurança dos *softwares* para evitar vazamentos e invasões.

III. Indique um encarregado para a segurança de dados (*DPO*) se sua empresa não se enquadrar nas exceções legais (microempresa, empresa de pequeno porte e startup) - como já apontado no capítulo anterior.

IV. Revise os contratos com fornecedores que tenham acesso aos dados da empresa, mesmo que de forma indireta. Altere as minutas contratuais para novos contratos e adite os contratos em curso para que fiquem de acordo com a legislação.

V. Invista em treinamentos para os colaboradores. A mudança de cultura, como já referido, é o maior desafio que as empresas enfrentarão para se adequarem à LGPD. Tal mudança não acontece imediatamente. É preciso dedicação tanto da gestão quanto do colaborador. Invista em workshops, palestras e debates com objetivo de mostrar ao colaborador o impacto que a LGPD terá em sua atividade e em como é importante sua colaboração para o sucesso da empresa em se adequar à lei.

A observação dessas cinco orientações básicas ajudará as organizações a iniciarem a jornada de adequação à LGPD e a se manterem no curso, antevendo eventuais problemas e desenvolvendo ferramentas para solucioná-los. Mas é importante saber essas regras não são imutáveis – e nem únicas.

Como o processo de adequação em si é uma jornada viva em constante mudança, as ferramentas e orientações de boas práticas de proteção de dados também devem acompanhar esse movimento. Portanto, dificilmente haverá uma fórmula única de trabalho que seja apta a todas as empresas.

A percepção da individualidade do negócio e dos *gaps* de segurança no controle de dados, bem como a capacidade de adaptação da organização serão elementos diferenciais para que a viagem pela LGPD seja mais branda e represente apenas progressos para as empresas.

IV. SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

A ANPD publicou um Guia orientativo de segurança da informação para agentes de tratamento de pequeno porte, sugerindo um checklist, do qual podem ser extraídos, dentre outros, os seguintes pontos:

⇒ POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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.

⇒ SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

- 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.
- Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais.
- 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.
- Inventariar e cifrar dados de dispositivos externos e armazená-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).

⇒ SEGURANÇA DAS COMUNICAÇÕES

- Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim-afim para serviços de comunicação.
- Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF – Filtro de Aplicação).
- Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e, integrar o antivírus ao sistema de e-mail.
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

⇒ DISPOSITIVOS MÓVEIS

Utilizar técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops.

Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível.

Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

⇒ CONSCIENTIZAÇÃO E TREINAMENTO

Realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD.

⇒ CONTROLE DE ACESSO

Implementar um adequado gerenciamento de senhas, estabelecendo controles tais como:

- evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos;
- utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos;
- não reutilizar senhas;

- Proibir o compartilhamento de contas ou de senhas entre funcionários;
- Aplicar o princípio do menor privilégio (*need to know*);
- Utilizar a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais.

⇒ GERENCIAMENTO DE CONTRATOS

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;
- Assinar termos de confidencialidade (*non-disclosure agreement - NDA*) com os funcionários da empresa.

⇒ GERENCIAMENTO DE VULNERABILIDADES

- Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores);
- Adotar e atualizar periodicamente *softwares* antivírus e *antimalwares*;
- Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

IMPORTANTE Esta Cartilha foi atualizada em dezembro de 2023
Coordenação Comissão Permanente Direito Digital e LGPD Marcela Joelsons
Coordenação da Divisão Jurídica da Federasul Fabiano Zouvi
Presidente da FEDERASUL Rodrigo Sousa Costa

Créditos

Benicia Montelli
Bruna Zani
Eliana Herzog
Erica Fabiana Mendes Grellert
Fabiana Lemos Marques
Fernanda Girardi
Flávia Coelho
Gabriela Glitz
Izabel Mello dos Santos
Júlia Klarmann
Marcela Joelsons
Letícia Batistela
Luciano Escobar
Niris Cristina Cunha
Roberta Feiten
Simone Rapone
Vladmir Bidniuk
Yago Oliveira