GUIA LGPD

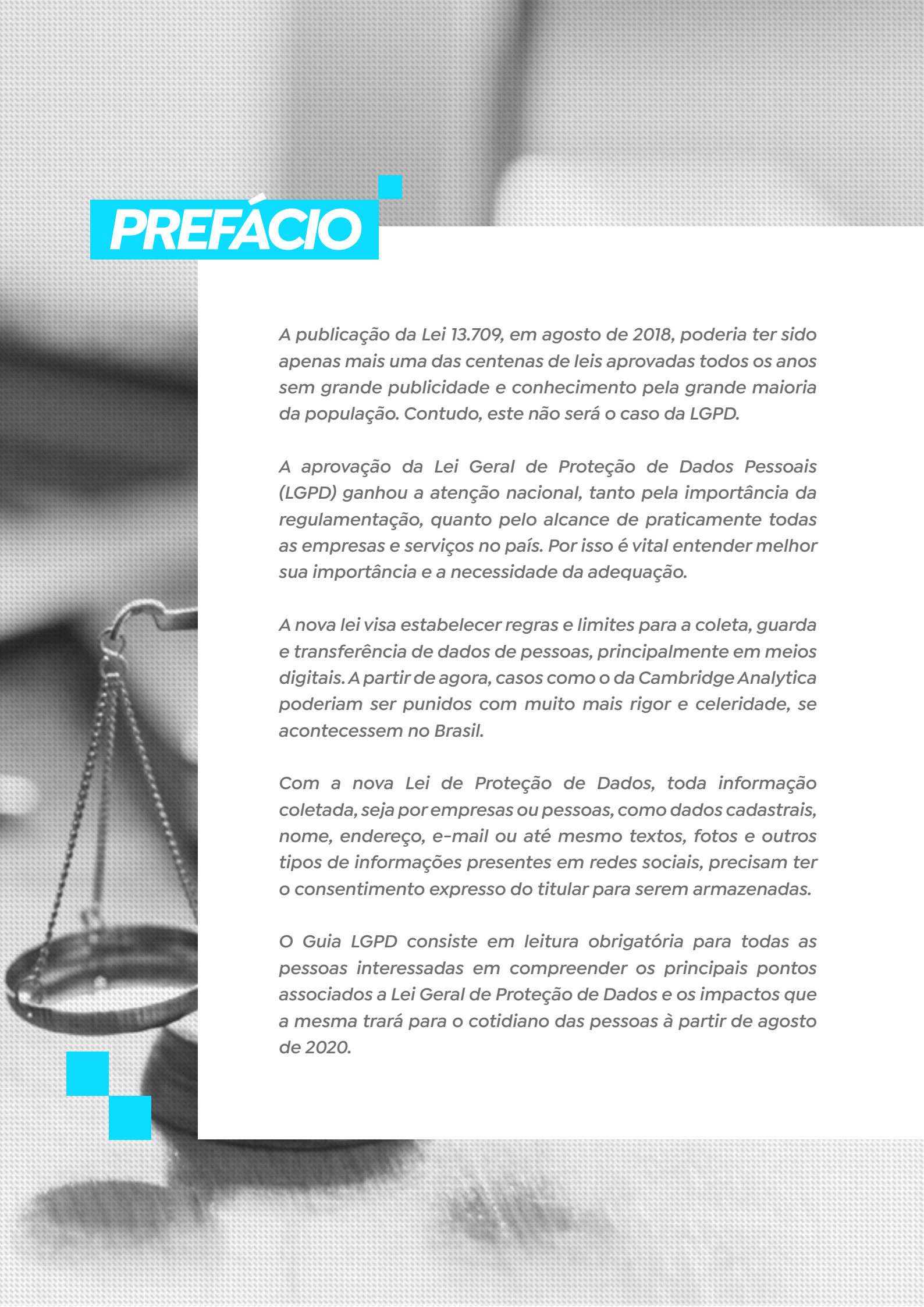
TUDO QUE VOCÊ PRECISA SABER SOBRE A LEI

ostec
Segurança digital de resultados

O Guia LGPD consiste em leitura obrigatória para todas as pessoas interessadas em compreender os principais pontos associados à Lei Geral de Proteção de Dados e os impactos que a mesma trará para o cotidiano das pessoas à partir de setembro de 2020

ÍNDICE

PREFÁCIO



A publicação da Lei 13.709, em agosto de 2018, poderia ter sido apenas mais uma das centenas de leis aprovadas todos os anos sem grande publicidade e conhecimento pela grande maioria da população. Contudo, este não será o caso da LGPD.

A aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD) ganhou a atenção nacional, tanto pela importância da regulamentação, quanto pelo alcance de praticamente todas as empresas e serviços no país. Por isso é vital entender melhor sua importância e a necessidade da adequação.

A nova lei visa estabelecer regras e limites para a coleta, guarda e transferência de dados de pessoas, principalmente em meios digitais. A partir de agora, casos como o da Cambridge Analytica poderiam ser punidos com muito mais rigor e celeridade, se acontecessem no Brasil.

Com a nova Lei de Proteção de Dados, toda informação coletada, seja por empresas ou pessoas, como dados cadastrais, nome, endereço, e-mail ou até mesmo textos, fotos e outros tipos de informações presentes em redes sociais, precisam ter o consentimento expresso do titular para serem armazenadas.

O Guia LGPD consiste em leitura obrigatória para todas as pessoas interessadas em compreender os principais pontos associados a Lei Geral de Proteção de Dados e os impactos que a mesma trará para o cotidiano das pessoas à partir de agosto de 2020.

INTRODUÇÃO

O QUE É LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709), que entrou em vigor em setembro de 2020, institui novas regras para a proteção de dados pessoais no país.

O novo regulamento foi fortemente inspirado no General Data Protection Regulation (GDPR), regramento de proteção de dados na União Europeia.

Mas, afinal, a quem se aplica a LGPD? Segundo o artigo 3o da lei, para toda pessoa natural (física) ou jurídica (de direito público ou privada) que: a) realize qualquer forma de tratamento de dados pessoais em território nacional; b) que efetue tratamento cujo objetivo seja o fornecimento de bens ou serviços de indivíduos localizados no território nacional; ou c) os dados tenham sido coletados no Brasil. Dessa forma pessoas físicas que prestam serviços, como contadores, médicos, corretores, etc, também precisarão adequar-se.

Uma vez compreendido para quem a lei se aplica, cumpre elucidar que dado pessoal é toda informação que identifica ou possa identificar uma pessoa natural. Além disso, a lei também delimitou a existência de dados sensíveis, que são informações pessoais como origem racial, crença, religião, liação partidária e sindical, dados relacionados à saúde, vida sexual, dados genéticos e biomédicos. Para esse segundo conceito, aplicou regras mais rigorosas de restrição ao tratamento, com o intuito de aumentar a proteção e evitar o uso discriminatório dos dados.

Em uma breve síntese, a LGPD passa a fornecer aos titulares mais autonomia e controle sobre o seus próprios dados pessoais, outorgando-lhes direitos como a transparência sobre o tratamento dos dados, renunciar a qualquer tempo ao tratamento dos dados, conhecimento claro sobre a finalidade do tratamento dos dados. Isso visa garantir ao titular a autodeterminação informativa com relação às suas informações pessoais.

Esse fortalecimento aos direitos individuais e da personalidade representa quebra importante de hábitos relacionados ao uso de dados pessoais. Empresas e pessoas que efetuam o tratamento de dados precisarão implementar importantes mudanças e para isso, conhecer a nova lei é indispensável. Vejamos.

PRINCÍPIOS GERAIS

Não há dúvida que a criação da LGPD está estreitamente relacionado ao princípio constitucional da privacidade. A lei, além de prever que todo o tratamento deve observar a boa-fé ainda pontuou os 10 princípios:

FINALIDADE_ realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ADEQUAÇÃO_ compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

NECESSIDADE_ limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

LIVRE ACESSO_ garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

QUALIDADE DOS DADOS_ garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da fanalidade de seu tratamento;

TRANSPARÊNCIA_ garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a

realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

SEGURANÇA_utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PREVENÇÃO_adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

NÃO DISCRIMINAÇÃO_impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS_ demonstração, pelo agente, da adoção de medidas e cazes eficapazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

BASES LEGAIS

A lei expressamente pontuou 10 hipóteses autorizadoras para o tratamento de dados pessoais e atribuiu à elas o nome da bases legais. Dessa forma, todo e qualquer tratamento somente poderá ser efetuado se pautado em uma das bases legais:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei no 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

DIREITOS AOS TITULARES

A LGPD previu expressamente certas garantias que o tratamento de dados deve assegurar aos titulares. É assegurado ao titular o direito ao acesso facilitado sobre os dados tratados, lhes informando a finalidade, forma e duração do tratamento, identificação e dados de contato do controlador, se há compartilhamento de informações, responsabilidade dos agentes.

Além disso deve permitir ao titular:

I - a confirmação da existência de tratamento;

II - o acesso aos dados;

III - a correção de dados incompletos, inexatos ou desatualizados;

IV - a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviços ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - a revogação do consentimento, nos termos do § 5o do art. 8o desta Lei.

FISCALIZAÇÃO DA LEI / SANÇÃO

O descumprimento das obrigações poderão ensejar questionamentos e ações por parte dos titulares, mas essa não é a única maneira das empresas responderem pelo tratamento ilegal de dados. A lei previu a criação da Agência Nacional de Proteção de Dados (ANPD) que, entre outras competências, irá fiscalizar a atividade do tratamento dos dados no país, exigir a apresentação de relatórios e informações, bem como aplicar eventuais penalidades.

A multa é sempre a sanção que causa mais impacto, ainda mais no elevado montante previsto pela lei, que poderá ser aplicada em até 2% sobre o faturamento da pessoa jurídica, limitada no total a R$ 50.000.000,00 (cinquenta milhões de reais) por cada infração.

A multa não é a única penalidade imposta pela lei, existe ainda a possibilidade de imposição de outras medidas, como publicização da infração, bloqueio e eliminação de dados pessoais. Estas são as possíveis obrigações que podem ser impostas pela autoridade.

No Brasil, além da ANPD, outras instituições exercerão a função de fiscalizadores, e por consequência também poderão aplicar multas e outras sanções, que é o caso do Ministério Público Estadual, Ministério Público Federal e Procon. No caso de tais entidades, as ações poderão requerer indenizações sobre danos coletivos, cujas multas podem ser ainda mais elevadas, além de medidas criminais.

SEGURANÇA DE DADOS PESSOAIS, GOVERNANÇA E BOAS PRÁTICAS

A LGPD consolidou obrigações a agentes de tratamento, como a adoção de medidas técnicas e administrativas de segurança, que visam proteger os dados pessoais de acessos não autorizados e evitam incidentes que resultam em perda, dano, alteração ou qualquer tratamento inadequado ou ilícito. A Autoridade Nacional ainda poderá indicar padrões técnicos mínimos para atendimento à tal obrigação.

Foi determinado ainda que o controlador deverá comunicar à Autoridade Nacional caso ocorra incidente que possa acarretar risco ou dano relevante aos titulares.

Por outro lado, a nova lei veiculou a instituição de políticas de governança e boas práticas, através da criação de regras que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas. Essas práticas deverão ser estimuladas pela ANPD e deverão ser consideradas em caso de aplicação de multas ou outras sanções.

PORQUE SUA EMPRESA DEVE SE ADEQUAR

Conforme visto acima, são muitos os direitos dos titulares que deverão ser resguardados pelos agentes de tratamento dos dados pessoais. Além daqueles, não é demais mencionar que uma vez capturados os dados, a empresa tem o dever da guarda e qualquer incidente de vazamento, perda, compartilhamento dessa informação poderá ensejar em responsabilidades.

O processo de adequação às exigências da lei pode ser moroso e complexo, a depender da maturidade em segurança digital e em tratamento de dados que a empresa possui. Além disso, outros fatores podem agregar complexidade ao processo, tais como: o seg-

mento de atuação, número de setores que tratam dados pessoais e volume de dados existentes.

Mas a aplicação de multas e outras sanções não deve ser o único propulsor para implementação por parte das empresa. A revisão dos fluxos de trabalho da empresa e a implementação de uma nova cultura de proteção de dados certamente será um importante e excelente diferencial competitivo, especialmente diante dos titulares dos dados (clientes, parceiros e colaboradores).

COMO SE ADEQUAR A LEI

O processo de adequação às exigências da lei pode ser relativamente rápido ou muito demorado, a depender da maturidade de segurança da informação e proteção de dados enfrentada da empresa.

PREPARAÇÃO / ETAPA INICIAL / ATOS PREPARATÓRIOS

É importante destacar que os proprietários, gestores, diretores, lideranças das empresas precisam ser os primeiros a compreender a necessidade do processo de transformação a ser implementado, seja para destinar parte do investimento necessário, ou para garantir engajamento da equipe para buscar melhores resultados.

Antes de iniciar a implementação é importante que a empresa identifique um responsável interno por todo o processo, que pode figurar como encarregado (um dos agentes de tratamento impostos pela lei), bem como um grupo de trabalho multidisciplinar que participará ativamente da próxima etapa chamada de Data mapping.

DATA MAPPING

Feito isso, é chegada a hora de iniciar um processo completo do mapeamento de todos os dados pessoais que estão sendo tratados na empresa. Note que esses dados também devem ser apurados ainda que estejam armazenados em meio físico (papel) ou off line (uma planilha na área de trabalho, por exemplo).

Esta é uma etapa que pode demandar tempo elevado, a depender do modelo de negócio, forma de organização das informações e uso de ferramentas para mapeamento dos dados na empresa. O data mapping deve ser realizado com elevado grau de minucia, para evitar omissões que causem prejuízos a organização. A utilização de uma metodologia estruturada, guiada por profissionais com experiências nas áreas de proteção de dados e segurança da informação resultará em um processo mais célere, seguro e eficiente.

O resultado desta etapa é o levantamento de todas as inconformidades identificadas na empresa, ou seja, todos os pontos em que não estão sendo cumpridas as obrigações impostas pela LGPD e outras legislações atreladas.

IMPLEMENTAÇÃO

Com esse levantamento é hora de iniciar todos os ajustes necessários para adequação, sejam eles nas esferas administrativas (mudança cultural), documental (contratos, termos de uso, políticas de privacidade), estruturais (sistemas, redes, restrição de acessos), etc.

Nesta etapa todos os dados pessoais tratados pela empresa deverão passar por adequações, se necessárias, para garantir essencialmente: a utilização de uma base legal, o respeito aos princípios previstos na lei e o atendimento dos direitos dos titulares.

RELATÓRIO DE IMPACTO

A LGPD impõe a obrigação da elaboração do Relatório de Impacto que é a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Portanto, feitas as correções pela empresa, é hora de elaborar o Relatório Impacto (documento indispensável em caso de fiscalização).

MONITORAÇÃO

Após essa etapa, é necessário multiplicar as boas práticas por toda a empresa. Para isso, a realização de treinamentos e eventos de conscientização focados em segurança da informação e proteção de dados pessoais é imprescindível, garantindo a continuidade da nova cultura. A implementação de políticas de governança, além de ser uma prática positiva internamente para a empresa, será considerada uma iniciativa positiva, em caso de fiscalização ou atuação, pela Agência Nacional de Proteção de Dados.

Porêm, não se pode esquecer que o dinamismo das corporações pode resultar no resgate de velhas práticas, implicando em novas violações às normas de proteção de dados pessoais. Razão pela qual, evidencia-se a importância da revisão contínua do ciclo de vida dos dados na empresa.

GLOSSÁRIO

Para melhor compreender a lei concentramos neste Glossário alguns dos conceitos mais importantes:

DADO PESSOAL_informação relacionada a pessoa natural identificada ou identificável;

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;

DADO ANONIMIZADO_dado relativo a titular que não possa ser identi cado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

TITULAR_pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

BANCO DE DADOS_conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

CONTROLADOR_pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

OPERADOR_pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

ENCARREGADO_pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

AGENTES DE TRATAMENTO_o controlador e o operador;

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

ANONIMIZAÇÃO_utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

CONSENTIMENTO_manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

TRANSFERÊNCIA INTERNACIONAL DE DADOS_transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

USO COMPARTILHADO DE DADOS_comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

RELATORIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS_documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

ÓRGÃO DE PESQUISA_órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

AUTORIDADE NACIONAL_órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados