DIREITO CONNECT

GUIA BÁSICO DE ADEQUAÇÃO À LGPD

LGPD APLICADA

INTRODUÇÃO

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD),

ou Lei nº 13.709/2018, que regulamenta o tratamento dos dados pessoais no Brasil, inclusive digitais, entrou em vigor em setembro de 2020, e suas penalidades pelo seu descumprimento passaram a ser aplicáveis a partir de 01/08/2021. Importante saber que a LGPD se aplica a todas as empresas privadas e públicas de todos os setores da economia e à administração pública, que realizem o tratamento de dados pessoais e/ou dados sensíveis, o que inclui sua coleta, armazenamento e descarte, entre outros.
Assim, nasce a necessidade de implementação dos princípios e normas da LGPD também na rotina das organizações,o que deve ser traduzido tanto na adequação de contratos e segurança dos dados de clientes, como em mudanças internas, ou seja, adequação do processo seletivo para novas vagas, processo de contratação, adoção de políticas de proteção de dados, Código de Ética, entre outros.
Por esse motivo, esse Guia tem por objetivo apresentar o que você precisa saber para adaptar seu negócio à Lei Geral de Proteção de Dados Pessoais.
Esse documento traz, a seguir, uma noção básica do que é necessário modificar/adequar/corrigir/implementar em sua organização para que você esteja em conformidade com a LGPD.

DIREITO CONNECT

PROGRAMA DE GOVERNANÇA E BOAS PRÁTICAS DE TRATAMENTO DE DADOS PESSOAIS

O PROGRAMA DE GOVERNANÇA E BOAS PRÁTICAS DE TRATAMENTO DE DADOS PESSOAIS

consiste em um conjunto de ações e políticas sugerido pela LGPD para demonstrar o comprometimento da empresa com os direitos dos titulares de dados pessoais e comprovar a adequação à LGPD.

Entendemos que o esse Programa deve contemplar ao menos 4 etapas:

1

IMPLEMENTAÇÃO

2

DPO

3

CAPACITAÇÃO

4

AUDITORIA

DIREITO CONNECT

1

IMPLEMENTAÇÃO

A PRIMEIRA ETAPA,

do Programa de Governança e Boas Práticas de Tratamento de Dados Pessoais tem por foco a reestruturação de comportamentos e documentos com finalidade de adequar a empresa à LGPD, o que contempla, ao menos, as ações que traremos a seguir.

Mas, antes disso, precisamos entender alguns conceitos:

DADO PESSOAL

Dados pessoais são quaisquer informações que identifiquem uma pessoa. Ex.: nome, CPF, RG, CNH, entre outros.

DADOS PESSOAIS SENSÍVEIS

Dentro da categoria de dados pessoais, os dados pessoais sensíveis são exclusivamente as informações relacionadas à 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 vinculadas a uma pessoa física.

DIREITO CONNECT

TRATAMENTO DE DADOS PESSOAIS

Tratamento de dados pessoais é toda e qualquer operação com dados pessoais. Alguns exemplos: coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação.

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.

DIREITO CONNECT

AÇÕES

MAPEAMENTO DE DADOS

Esta ação tem por objetivo identificar se a empresa trata dados, quais dados são tratados e de que forma são tratados.

Será necessário entender o fluxo de cada dado pessoal tratado dentro da empresa, ou seja, você precisará mapear os dados tratados e relacionar quem coleta dados, como é feita esta coleta, quem tem acesso a esses dados, onde são armazenados, se são compartilhados com outras empresas, por quanto tempo ficam armazenados e como são descartados.

POLÍTICA E CÓDIGO DE ÉTICA

Esta ação tem por objetivo implantar, deixar explícito e garantir a executividade da proteção de dados como um valor da empresa.

É necessário que a proteção de dados passe a ser um valor da empresa e uma conduta esperada de todos os colaboradores e sócios. Por isso, é indispensável que seja criada uma Política de Proteção de Dados Pessoais e um Código de Ética que deverão ser disponibilizados a todos os empregados, assim como se faz com o Manual do Colaborador.

DIREITO CONNECT

REESTRUTURAÇÃO DE CONTRATOS INTERNOS E EXTERNOS

Esta ação tem por objetivo garantir o atendimento ao princípio da transparência trazido pela LGPD.

Outra importante mudança se dará nos contratos internos e externos da empresa, haja vista que a LGPD tem como um de seus princípios a transparência, motivo pelo qual o indivíduo deverá ter pleno conhecimento de que seus dados serão tratados, para qual finalidade e que a empresa adota medidas que garantem sua proteção.

Dessa forma, contratos com seus clientes ou com fornecedores deverão conter cláusulas sobre tratamento de dados pessoais, que precisarão informar que os dados são tratados para determinado propósito e apresentar as obrigações da empresa com relação à proteção desses dados.

Assim como, contratos internos que envolvem a relação empresa x empregados ou empresa x terceirizados, deverão de igual maneira apresentar cláusulas sobre tratamento de dados pessoais.

PROCEDIMENTOS RH

Esta ação tem por objetivo garantir a transparência, assim como proteção de dados pessoais de candidatos a vagas.

Um ponto importante que merece ser apresentado nesse guia é a necessidade de adequação de processos de Recursos Humanos que precisarão ser revistos de modo a preservar a privacidade e outros direitos dos titulares de dados pessoais, nesse caso os candidatos.

DIREITO CONNECT

Dessa maneira, o processo de recebimento de currículos, entrevistas, armazenamento de dados do candidato deverão estar de acordo com a LGPD, bem como o tratamento de dados deverá ser transparente ao candidato.

DATA PROCESSING AGREEMENT – DPA (CONTRATO COM PROCESSADOR)

Esta ação tem por objetivo regular a relação Controlador x Operador.

Ainda, entende-se como um relevante instrumento para demonstrar que a empresa se preocupa com os direitos dos titulares de dados, que ela firme contratos com os operadores de dados, ou seja, terceiros que acabam tratando dados pessoais coletados pela empresa e em nome dela.

Citamos como exemplo a empresa que lhe presta serviços de software de gestão, provavelmente você fornece dados dos seus clientes para ela, ao armazenar esses dados no sistema. Nesse caso, é importante que haja um contrato que delimite as responsabilidades de cada um nesse processo e o respeito à privacidade e outros direitos dos titulares de dados.

PLANO DE RESPOSTA À INCIDENTES DE DADOS PESSOAIS

Esta ação tem por objetivo garantir o dever de comunicar a ANPD quando acontecer incidentes com dados pessoais.

O Plano de Resposta a Incidentes consiste em um documento interno da empresa que deve ser amplamente conhecido por todos e que dispõe sobre as medidas que devem ser tomadas no caso de um Incidente de Segurança em Dados Pessoais, como por exemplo, vazamento de dados. Esse Plano deverá apontar os responsáveis por cada ação e quais serão os procedimentos adotados.

DIREITO CONNECT

2

DPO

A LGPD IMPÕE COMO OBRIGAÇÃO ÀS EMPRESAS A NOMEAÇÃO DE UM DPO

Você poderá apontar alguém interno, como também poderá contratar prestador de serviço especializado.

O DPO (encarregado) é a pessoa natural indicada pelo controlador responsável por fazer a comunicação entre controlador, titulares e autoridade nacional.

A identidade e as informações de contato do DPO deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site da empresa.

O DPO deverá ser responsável pelas seguintes atividades:

ACEITAR RECLAMAÇÕES DOS TITULARES,

prestar esclarecimentos e adotar providências;

RECEBER COMUNICAÇÕES

da Autoridade Nacional de Proteção de Dados Pessoais - ANPD

DIREITO CONNECT

ORIENTAR OS FUNCIONÁRIOS E OS CONTRATADOS DA ENTIDADE

da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; ento, arquivamento, armazenamento, eliminação.

EXECUTAR AS DEMAIS ATRIBUIÇÕES

determinadas pelo controlador ou estabelecidas em normas complementares..

AINDA, CABERÁ AO DPO ELABORAR O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD,

que é um documento que averigua os riscos do tratamento de dados pessoais e apresenta mecanismos para redução ou eliminação desses riscos. Este relatório, em determinados casos, poderá ser exigido pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que é órgão responsável pela fiscalização da LGPD.

DIREITO CONNECT

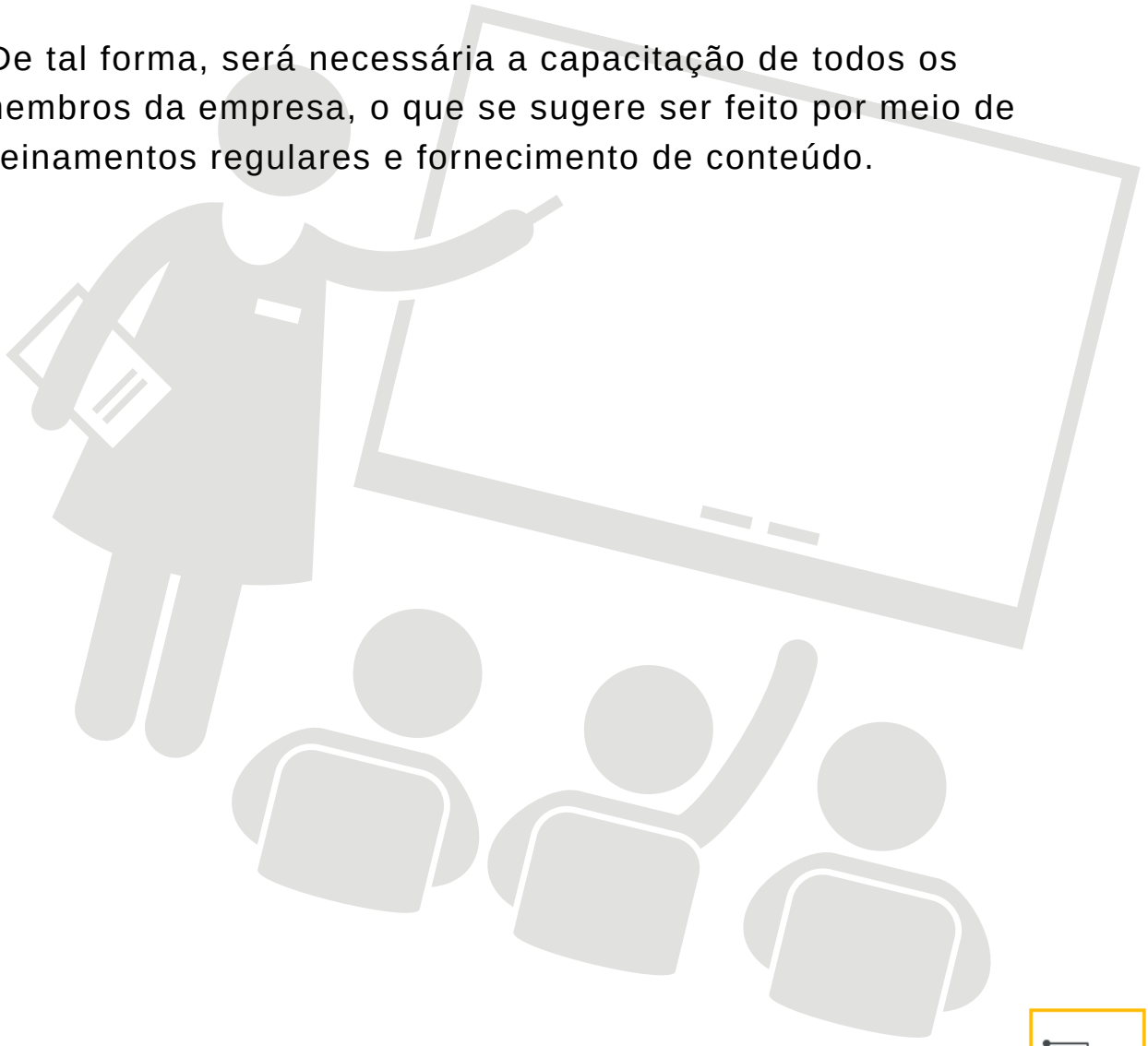
3

CAPACITAÇÃO

CONFORME JÁ MENCIONADO,

a proteção e dados deverá ser uma conduta esperada de todos da empresa, empregados, sócios ou terceirizados. Desse modo, somente é possível exigir o cumprimento das políticas de tratamento de dados se todos conhecerem a LGPD.

De tal forma, será necessária a capacitação de todos os membros da empresa, o que se sugere ser feito por meio de treinamentos regulares e fornecimento de conteúdo.



DIREITO CONNECT

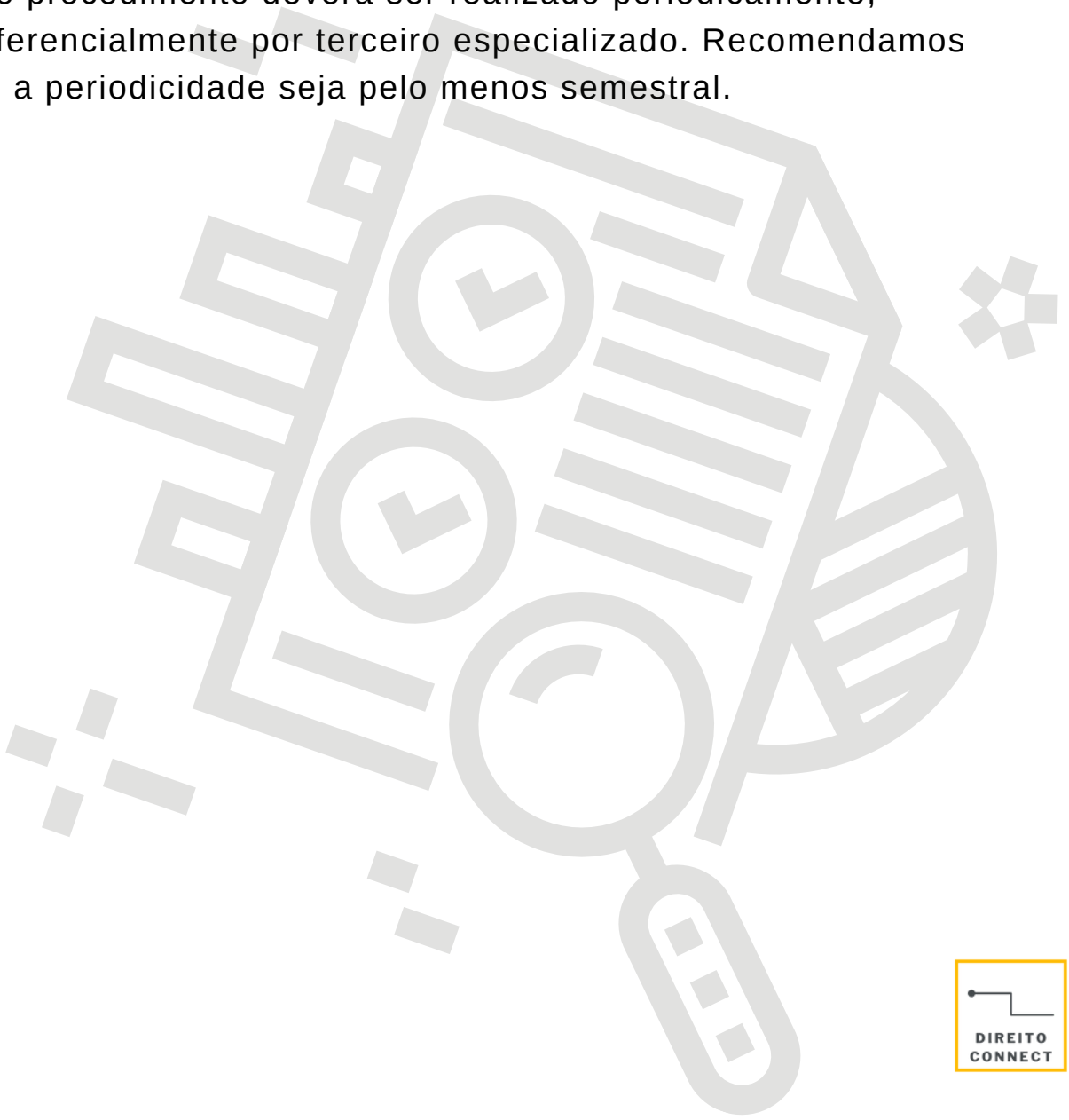
4

AUDITORIA

A AUDITORIA DO PROGRAMA DE GOVERNANÇA E BOAS PRÁTICAS DE TRATAMENTO DE DADOS PESSOAIS

permite que a empresa possa melhorar processos, encontrar falhas e demonstrar à ANPD seu comprometimento.

Este procedimento deverá ser realizado periodicamente, preferencialmente por terceiro especializado. Recomendamos que a periodicidade seja pelo menos semestral.



DIREITO CONNECT

CONCLUSÃO

A LGPD INSTITUIU NOVOS CONCEITOS, PRINCÍPIOS, DIREITOS E OBRIGAÇÕES QUE, EM CONJUNTO,

traduzem uma nova cultura de mercado nas operações com dados pessoais, de maior transparência e segurança, bem como autonomia do titular de dados.

Com a entrada em vigor desta lei, as empresas se obrigam a tratar os dados pessoais apenas para fins do negócio, precisam controlar o acesso e manipulação aos dados e oferecer garantias de segurança do armazenamento destes dados aos titulares que os forneceram.

O assunto é extenso, mas esperamos que esse material possa contribuir para a disseminação de conhecimento dos principais tópicos da LGPD, mas caso precise de maiores informações você poderá conversar conosco.

DIREITO CONNECT


DIREITO
CONNECT