LEI GERAL DE PROTEÇÃO DE DADOS
GUIA PARA CONFORMIDADE COM A LEI

SINDIMETAL-PR

Sistema Fiep FIEP

Índice

Lei Geral de Proteção de Dados - Bases Legais 6

Projeto de Conformidade com a Lei Geral de Proteção de Dados 7

1. Autoanálise 7
2. DPO – Encarregado de Dados 10
3. Gestão de Dados 14
4. Gestão de Processos 17
5. Minutas Contratuais 18
6. Tecnologia 21
7. Gestão da Mudança 24

Introdução

Por que a LGPD existe? Em um mercado global, onde cada vez mais a informação é o ativo mais precioso para as empresas, uma tendência desenfreada de coleta de dados foi instaurada. Com isso, diversas economias internacionais iniciaram uma regulamentação no trato de dados pessoais. A Lei Geral de Proteção de Dados é uma resposta do Brasil para o mundo, demonstrando o comprometimento das empresas que operam no Brasil com a privacidade de seus clientes, colaboradores e parceiros de negócio. Antes de mais nada, gostaríamos de passar alguns conceitos para o entendimento da legislação:

Dados pessoais: toda informação relacionada à pessoa identificada ou identificável – como RG, CPF, nome, estado civil, dados de localização (GPS), entre outros;

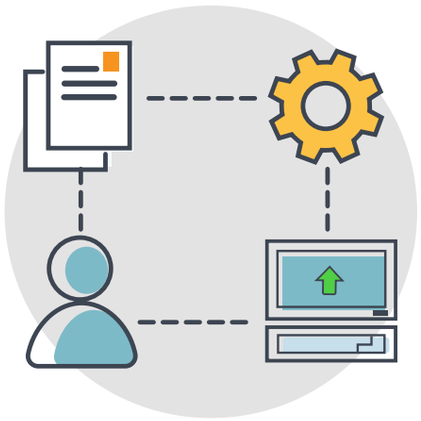
Dados pessoais sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicatos ou às organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos;

Penalidades: advertência; multa de até 2% do faturamento da pessoa jurídica ou grupo econômico, limitado em R$ 50 milhões – por infração; Publicação da infração (danos reputacionais); bloqueio/eliminação dos dados referentes à infração; possibilidade de suspensão das atividades exercidas;

Titular dos dados: pessoa natural a quem pertence os dados;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete 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;



Direitos dos titulares:

- Confirmação do tratamento, acesso e correção dos dados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com a lei;
- Portabilidade a outro fornecedor;
- Informação das entidades públicas e privadas com as quais o controlador compartilhou os dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento ao tratamento.

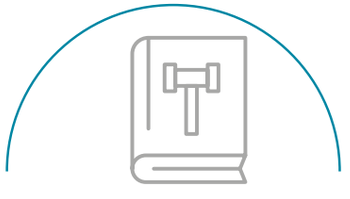
Lei Geral de Proteção de Dados - Bases Legais

1 Cumprimento de Obrigação legal

2 Execução de políticas públicas

3 Estudo por Órgão de Pesquisa

4 Execução de contrato



5 Exercício Regular de Direitos

6 Projeção da Vida

7 Tutela de Saúde

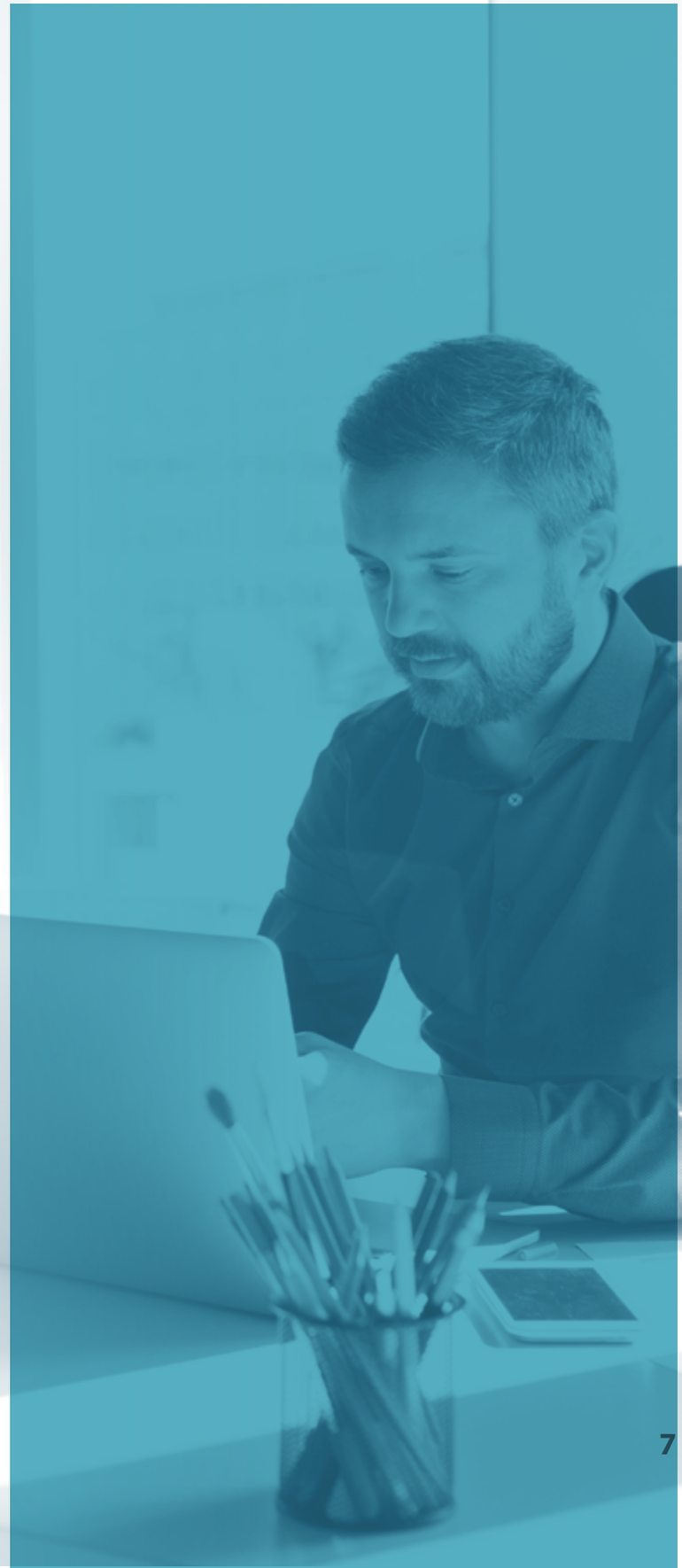
8 Legítimo Interesse

9 Proteção ao Crédito

10 Consentimento

O Sistema Fiep, em parceria com os sindicatos, tem a missão de trazer para você, indústria associada, não apenas os conceitos básicos presentes na lei, mas sim uma abordagem prática do que devemos realizar para estar em conformidade com a lei.
A seguir, apresentamos um modelo básico para esta conformidade mínima. Leia com atenção! Esperamos que seja de grande utilidade.

PROJETO DE CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS



1. Autoanálise

De qual área da empresa a LGPD é a responsabilidade? Bom, por ser uma lei, a responsabilidade é do jurídico, correto? Mas temos tantas necessidades em tecnologia, então é da TI, certo? Porém, a maior parte dos dados coletados são de colaboradores, então é do RH, né? Lendo a lei algumas vezes, é possível ver que se trata de integridade, então é com o compliance, isso? A resposta para todas as perguntas é: não. Um projeto de conformidade a Lei Geral de Proteção de Dados com uma única área envolvida está fadado a ser incompleto.

A primeira situação que devemos entender é que a nova lei irá permear por todas as áreas da organização. E a melhor forma de iniciarmos este engajamento é obtendo o apoio da alta administração. A cultura de exemplo é viva nas organizações, sendo assim, apresente a lei aos seus executivos, esse é o primeiro público a ser conscientizado. Com algumas leituras sobre a lei - sim, uma única leitura não trará clareza o suficiente -, a decisão é: esse trabalho será conduzido pelo time interno ou devemos contratar uma consultoria especializada para tal? Não existe resposta certa ou errada para essa pergunta, um trabalho conduzido por colaboradores é profundo e menos custoso. Uma consultoria especializada, pode ser mais ágil e assertiva nos planos de ação.

Caso opte pela condução interna, um aviso: esse trabalho exige dedicação. Com a incumbência de auxílio, confira algumas sugestões de atividades a serem seguidas e frentes de trabalho mapeadas. Lembre-se: o presente guia tem como objetivo clarificar etapas de um projeto, conforme o seu tipo de operação, outras etapas serão necessárias.

2. DPO – Encarregado de Dados

ARTIGO 9 ➡ CANAL DE ATENDIMENTO DO DPO
ARTIGO 18 ➡ COMPLEMENTAR AO 9
ARTIGO 19 ➡ COMPLEMENTAR AO 9
ARTIGO 11 ➡ HIPÓTESES PARA TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
ARTIGO 41 ➡ NOMEAÇÃO DPO
ARTIGO 48 ➡ COMUNICAÇÃO DE INCIDENTE COM DADOS
ARTIGO 50 ➡ GOVERNANÇA DE DADOS

A GDPR tem na figura do DPO (Data Protection Officer) o responsável pelas diretrizes de tratamento de dados nas organizações - a LGPD tem a mesma figura, nomeada como Encarregado de Dados. Após a primeira etapa, a autoanálise, compete a organização avaliar onde o Encarregado de Dados melhor se encaixa, podendo ser: um colaborador, uma área ou um terceiro especializado. Isso mesmo, a lei determina no artigo 41 que o controlador deve nomear o Encarregado de Dados e publicar essa nomeação, mas não determina que o mesmo deva ser uma pessoa natural.

Para melhor direcionar sua análise de quem deve assumir esta (grande) tarefa, pontuamos algumas responsabilidades do Encarregado:

a. Educar a empresa e os funcionários sobre requisitos de conformidade importantes;

b. Treinamento e posicionamentos para o pessoal envolvido no processamento de dados;

c. Interagir com a Autoridade Nacional de Proteção de Dados;

d. Manter registros abrangentes de todas as atividades de processamento de dados realizadas pela empresa, incluindo o objetivo de todas as atividades de processamento, que devem ser tornadas públicas mediante solicitação;

e. Interface com os titulares de dados para informá-los sobre como os seus dados estão sendo usados, seus direitos de exclusão de dados pessoais e quais medidas a empresa adotou para proteger suas informações pessoais.

Este “porta bandeira” da privacidade terá um papel-chave durante o seu projeto de conformidade à LGPD, além de obrigações recorrentes com a lei. Como explicado no item “e”, a interface com os titulares de dados será constante. A Lei Geral de Proteção de Dados indica que todas as organizações deverão dispor de um canal de atendimento para demandas de privacidade junto aos seus clientes. Esse canal pode ser um sistema dedicado, pode ser um formulário ou até um e-mail, mas ele deve existir. Recomendamos que revise a parte de “Direito dos Titulares”, explicada anteriormente em nosso guia, para que visualizem quais as possíveis demandas que serão atendidas pelo DPO.

Outro aspecto fundamental do Encarregado de Dados são os clientes mais próximos da organização: os seus colaboradores. Um profissional com independência necessária para realizar posicionamentos consultivos às áreas da empresa são essenciais: cabe ao encarregado de dados direcionar as áreas da organização e seus colaboradores com relação ao tratamento de dados, zelando pela privacidade e a conformidade com a LGPD. Sendo assim, uma dica adicional – recomendamos que o mesmo canal que utilizar para atendimento dos titulares dos dados, fique disponível para seus colaboradores demandarem consultivos do Encarregado de Dados.

3. Gestão de Dados

ARTIGO 6 ➡ PRINCÍPIOS DOS TRATAMENTOS DE DADOS
ARTIGO 7 ➡ HIPÓTESES DE TRATAMENTO DE DADOS
ARTIGO 37 ➡ INVENTÁRIO DE DADOS

A lei fala em proteção de dados pessoais, mas como iremos proteger os mesmos se não os identificamos? Sem dúvidas, a maior etapa do projeto – em tempo de execução, é o Inventário de Dados. E não, não tem como fugir. O artigo 37 deixa claro que toda empresa, no caráter de controlador ou operador deve manter o registro das suas operações de tratamento de dados. Pense o seguinte: caso indagado por um titular de dados, por um parceiro de negócio ou pela própria Autoridade Nacional de Proteção de Dados (ANPD), a empresa deverá responder quais dados são tratados em seus processos. Nessa etapa, recomendamos que toda a organização faça parte do projeto.

Cabe ao time do projeto entrevistar todas as áreas e entender quais os processos que contemplam dados pessoais. O seu inventário deve conter, no mínimo, a seguinte estrutura:

a. Mapeamento indicando o processo, empresa responsável (pensando em um grupo empresarial, qual dessas tem acesso aos dados), quais dados são coletados, quem é o titular dos dados, para qual finalidade, onde esses dados são armazenados, quem tem acesso, por qual motivo esses dados são coletados e qualquer outra informação que sua organização acredite ser relevante para maior compreensão deste mapeamento;

b. Após o mapeamento dos dados, avalie qual a hipótese de tratamento embasa a coleta;

c. Aconselhamos que as empresas apliquem uma classificação do risco do tratamento para a organização, que pode ser dividido como "baixa, média e alta". O objetivo dessa classificação é criar uma priorização de quais os processos que apresentam maior risco de conformidade à empresa, e devem ser tratados primeiro.

Esse mapeamento deve existir, mas como ele será feito, depende de cada organização. Existem prestadores de serviço que ofertam soluções tecnológicas para tal, inclusive o Senai, mas qualquer forma de registro organizado é recomendada, principalmente, o "bom e velho" Excel. Adicionalmente, a melhor forma de registrar todo o mapeamento é por meio de entrevistas, um trabalho a quatro, oito, dezesseis mãos. Lembre-se: esse documento é vivo, de maneira constante, novos tratamentos irão começar na organização e sempre devem ser registrados no inventário.

4. Gestão de Processos

Esta etapa é uma consequência natural ao Inventário de Dados. Depois de entender todos os processos e tratamento de dados existentes na organização, priorizar os riscos de conformidade à LGPD em cada um desses, e como podemos tratá-los? Existem, dentre outras opções, duas formas claras: tecnologia (item 6 do nosso guia) e processos.

O processo pode ser revisitado para a diminuição desses riscos, buscando soluções práticas como:

a. Identificar se algum dos dados pessoais coletados excede a finalidade do processo, podendo ser retirado da coleta e excluído da base de dados;

b. Validação para a troca de ferramentas com o objetivo de envio de dados pessoais, que não apresentam segurança desejada;

c. Digitalização de documentos físicos com dados pessoais, arquivando em ambientes tecnológicos seguros;

d. Centralização de processos com dados pessoais sensíveis – remover do fluxo de informações pessoas que não participem diretamente do processo. Exemplo: colaboradores em excesso copiados no e-mail.

5. Minutas Contratuais

ARTIGO 7 – ITEM 4 ➡ O ARTIGO MOSTRA AS DEZ HIPÓTESES DE TRATAMENTO DE DADOS, E O ITEM VINCULA A CONTRATOS.
ARTIGO 8 ➡ O ARTIGO TRATA DE CONSENTIMENTO
ARTIGO 14 ➡ TRATAMENTO DE MENORES DE IDADE
ARTIGO 39 ➡ DETERMINAÇÃO CONTROLADOR X OPERADOR

Como comentamos anteriormente, a LGPD dispõe de dez hipóteses legais para o tratamento de dados pelas empresas, e uma delas é a execução de contrato. Em outras palavras, todo contrato celebrado entre as partes que registre o tratamento de dados pessoais e os discrimine, resguarda a empresa durante a vigência do mesmo.

Sendo assim, constatamos que os contratos firmados são de suma importância para a segurança jurídica da organização no que tange à LGPD, mas temos outros pontos importantes a destacar, são eles:

a. Revisite todas as minutas contratuais da empresa – inclua cláusulas de privacidade de dados, discriminando quais dados pessoais são coletados durante o processo, para qual finalidade são utilizados e por quanto tempo serão armazenados;

b. Coleta de dados que não são firmadas em contratos e não possuem outra hipótese legal para tratamento, devem ser suportadas por um Termo de Consentimento. Esse documento nada mais é do que uma autorização do titular dos dados para que esse tratamento possa ocorrer – vale salientar que o mesmo é revogável. O Termo de Consentimento deve firmar quais os dados são coletados, para qual finalidade, por quanto tempo serão armazenados e deve dispor de um canal de comunicação junto ao DPO da organização.

c. Caso o público alvo do Termo de Consentimento seja de menores de 18 anos, vale salientar que o consentimento só pode ser realizado por um dos pais ou responsável legal do menor;

d. Cabe ao operador de dados realizar o tratamento mediante as instruções do controlador. Por isso, caso a sua organização colete dados pessoais e compartilhe com parceiros de negócio, recomendamos que todas as instruções cabíveis sejam formalizadas em aditivos contratuais, definindo responsabilidades e criando transparência para a relação de tratamento de dados entre as partes. Lembre-se: seu parceiro de negócio é corresponsável pelo tratamento de dados perante à Autoridade Nacional de Proteção de Dados (ANPD).

6. Tecnologia

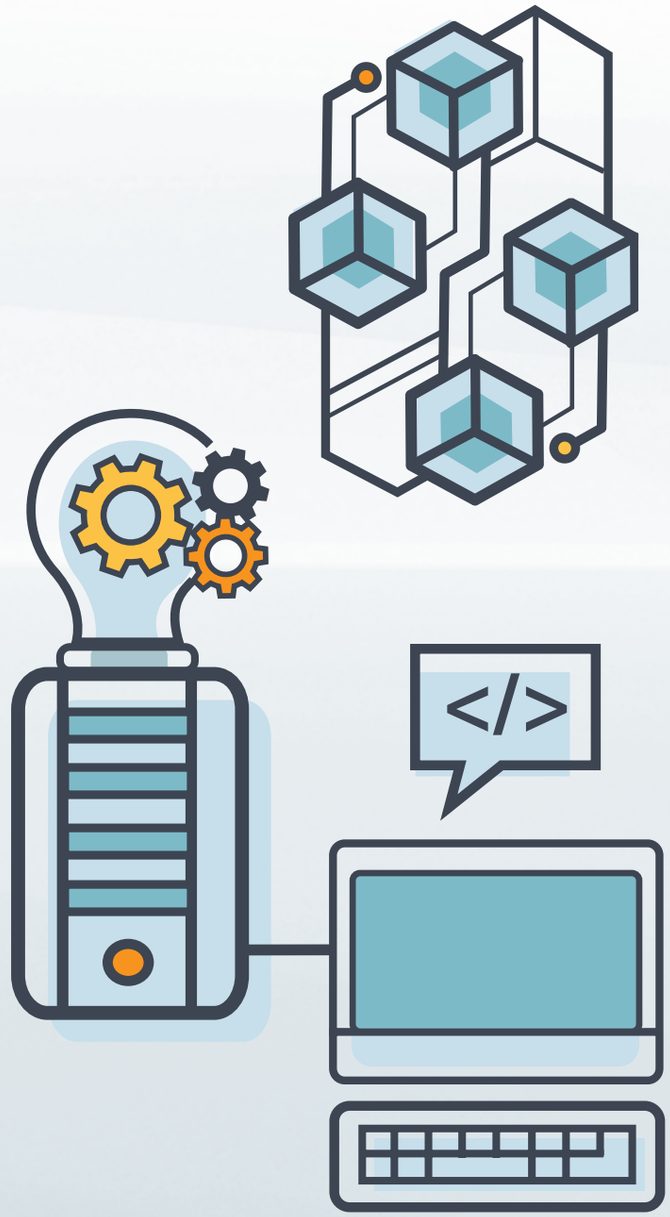
ARTIGO 6 – ITEM 7 ➡ O ART. 6º FALA SOBRE AS BOAS PRÁTICAS PARA O TRATAMENTO DE DADOS. NO ITEM 7, DE MANEIRA DIRETA, FALA-SE SOBRE A NECESSIDADE DE SEGURANÇA DE DADOS.
ARTIGO 12 ➡ ARTIGO DEDICADO À ANONIMIZAÇÃO DE DADOS
ARTIGO 46 ➡ ARTIGO DEDICADO À PROTEÇÃO DE DADOS PESSOAIS
ARTIGO 47 ➡ ARTIGO DEDICADO À SEGURANÇA DA INFORMAÇÃO, MESMO APÓS O TRATAMENTO DE DADOS
ARTIGO 49 ➡ ARTIGO DEDICADO A DEFINIR QUE SISTEMAS DEVEM SER ESTRUTURADOS NAS BOAS PRÁTICAS DE GOVERNANÇA, ACESSO E SEGURANÇA.

É importante frisarmos: independentemente do tipo de organização, hoje as maiores concentrações de dados são encontradas no ambiente tecnológico. Claro, qualquer tipo de relatório ou base sistêmica pode ser impresso, qualquer coleta de dados pode ocorrer via formulário físico, mas a realidade é que, tendo em vista que a lei tem como premissa a proteção de dados pessoais, o maior risco de vazamento está na esfera tecnológica.
Sendo assim, a LGPD é direta: as empresas devem investir e comprovar recursos e comprometimento com a segurança de dados pessoais de clientes, colaboradores ou parceiros de negócio. Mas como evidenciar essas atividades? Como transformar os artigos referenciados acima em ações? Vamos lá:

a. Todas as medidas de segurança tecnológica permeiam em um programa, nas boas práticas de mercado, chamado de SEGURANÇA DA INFORMAÇÃO. Referências de controles para um programa de segurança da informação satisfatório estão descritos na norma ISO/IEC 27701;

b. Definições de documentos normativos que orientem colaboradores e parceiros de negócio são essenciais – Política de Segurança da Informação, Política de Privacidade de Dados e Processos de Respostas a Incidentes;

c. Anonimização de dados – tornar um dado pessoal anonimizado é quando o mesmo deixa de ser identificável. Assim, em caso de vazamentos, os titulares dos dados não sofrem prejuízo algum. Existem ferramentas de mercado que auxiliam na anonimização de bases, altamente recomendável para empresas com um alto volume de dados pessoais sensíveis;



d. Com a LGPD, seu processo de contratação deve ser revisto. Fornecedores de sistemas e aplicativos devem comprovar certificações e capacidades técnicas de ofertar o produto contratado com segurança, tendo em vista que dados de colaboradores, clientes e parceiros de negócio serão armazenados nos mesmos;

e. Gestão de acessos – quanto menos pessoas tiverem acessos às bases de dados pessoais, menor a chance de vazamento. Sendo assim, invista em um processo que estruture uma gestão de acesso confiável na organização (com autorização para a concessão de acessos, com revisões periódicas). Apenas colaboradores ou terceiros, que tenham necessidade operacional, devem acessar bases de dados pessoais;

f. Controles tecnológicos – implementação de ferramentas tecnológicas como: firewalls, análises e vulnerabilidade e antivírus.

7. Gestão da Mudança

ARTIGO 41 – ITEM 3 ➡ O ITEM DESCREVE A IMPORTÂNCIA DE O ENCARREGADO DE DADOS ORIENTAR COLABORADORES SOBRE PRÁTICAS DE PRIVACIDADE.

O presente tópico é essencial para qualquer projeto de sucesso. Observamos que a LGPD irá alterar os contratos elaborados pelas empresas, modificando o modo que as empresas interagem com clientes, alterando o ambiente tecnológico das organizações. Mas qual o denominador comum em todos esses processos? Pessoas! Não importa o quanto as empresas invistam recursos físicos e operacionais para a proteção de dados, se os seus colaboradores não tiverem o engajamento com essa prática, o ambiente apresenta um risco considerável de vazamento.

O engajamento dos colaboradores tem algumas premissas. Antes de apontá-las, é importante dizer que este processo requer esforço e tempo, nenhuma cultura é transformada "de uma hora para outra". Aqui, listamos algumas ações para conscientização geral de todos da organização:

a. O engajamento dos líderes da empresa é essencial para que seus colaboradores vejam nos mesmo o exemplo;

b. Elaborar comunicados de conscientização periódicos para que todos se familiarizem com os termos da LGPD e suas práticas. Utilize o canal de comunicação que atinja a maioria dos colaboradores: e-mail, cartazes, folhas impressas em elevadores etc.

c. Criar um treinamento dedicado à Lei Geral de Proteção de Dados, com evidência de realização por colaborador – uma forma de evidenciar o comprometimento da companhia para a conscientização de todos;

d. Inclusão de um tópico dedicado a privacidade no Código de Conduta da organização. É importante frisar que o comprometimento com a privacidade é uma conduta desejada pelo corpo de colaboradores;

e. Aos poucos, deixe de referenciar a LGPD como norteador comportamental e adote termos como "Cultura de Privacidade" ou "Cultura Organizacional". A conformidade com a lei tem que deixar de ser uma obrigação e passar e ser comportamental, pensando na perpetuidade do assunto.

Por fim, mas não menos importante, todas as organizações possuem parceiros de negócio, alguns desses, essenciais para a operação de suas atividades. Como a Lei Geral de Proteção de Dados trata da corresponsabilidade entre Controlador e Operador (definições realizadas no início do documento), a conscientização dos parceiros de negócio torna-se tão importante quanto a de colaboradores. Identifique quais são os mais importantes e realize reuniões de discussão sobre o tema, buscando o engajamento de todos.

Este guia foi elaborado pelo Sistema Fiep, por meio da Fiep, em parceria com os sindicatos do estado do Paraná para fomentar o *compliance* com a Lei Geral de Proteção de Dados nas nas indústrias paranaenses. Com a nova legislação em vigor, falar sobre a privacidade de dados é fundamental para reforçar a confiabilidade entre as empresas e seus clientes.

Para auxiliar as instituições nesse processo, o Senai no Paraná oferta uma consultoria especializada no assunto, oferecendo apoio às indústrias paranaenses para a realização de um diagnóstico da situação atual da empresa em relação à LGPD.

Clique aqui e saiba mais sobre o serviço.

SINDIMETAL-PR

Sistema Fiep FIEP