Cartilha de

PROTEÇÃO E PRIVACIDADE DE DADOS

Sistema FIERGS
SESI | SENAI | IEL | CIERGS

LEI GERAL DE PROTEÇÃO DE DADOS

Lei nº 13.709 de 14 de agosto 2018 – Vigente desde 18 de setembro de 2020.

Cartilha atualizada até março de 2025.

Sumário

1. Introdução

A Lei Geral de Proteção de Dados – LGPD nº 13.709, sancionada em agosto de 2018, teve sua vigência assegurada em setembro de 2020 (Lei 14.058/2020), a partir de quando tornou-se necessário o trabalho de todos em prol da adequação às novas regras voltadas a proteção e tratamento de dados pessoais, considerando que toda interação com clientes, empregados, fornecedores e qualquer outro parceiro de negócios se dá a partir da coleta ou uso de dados, objeto da nova norma.

A LGPD estipula uma série de obrigações para empresas públicas ou privadas, com ou sem fins lucrativos, que realizem, dentre outras operações, o armazenamento, compartilhamento e eliminação de **dados pessoais**, seja online ou em meio físico, inclusive estabelecendo regras específicas para a transferência internacional de dados e, por isso, é de extrema importância que todas as empresas, independentemente de seu porte e segmento, estejam preparadas e munidas de informações para um efetivo processo de revisão e adequação das práticas de gestão à nova norma, avaliando os riscos, planejando as mudanças internas necessárias e se organizando para garantir a segurança de tais informações de forma transparente.

Em linhas gerais, os titulares de dados passarão a ter maior controle sobre todo o tratamento dos seus dados pessoais. Em vista disso, diversas obrigações decorrem para aqueles responsáveis pelo tratamento de dados pessoais.

Mesmo antes da possibilidade de aplicação de sanções administrativas, que iniciaram a partir de 01/08/2021, o Poder Judiciário e os órgãos governamentais setoriais de proteção aos direitos dos cidadãos (exemplo: Procon/Bacen/Anatel/Ministério Púbico) já se pautavam no direito à privacidade e na LGPD para aplicar eventuais condenações, em razão do descumprimento das legislações que preservam a proteção de dados e privacidade, aplicando

sanções judiciais por responsabilidade civil e outras sanções previstas em legislações anteriores, como por exemplo, a partir da Constituição Federal, do Código Civil, do Código de Defesa do Consumidor e do Marco Civil da Internet.

Por meio da promulgação da Emenda Constitucional nº 115/2022, o direito à proteção de dados pessoais entrou para o rol de direitos e garantias fundamentais do cidadão, previsto na Constituição Federal.

O texto, incluído no inciso LXXIX, do artigo 5º da Constituição Federal, assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive em meios digitais, garantindo a privacidade dos indivíduos, além de trazer maior segurança jurídica ao país na aplicação da Lei Geral de Proteção de Dados.

Também foram incluídos os incisos XXVI e XXX, respectivamente, aos artigos 21 e 22 da Carta Magna, atribuindo à União competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, bem como competência privativa para legislar sobre a matéria, afastando o risco de iniciativas legislativas de estados e municípios na interferência de aplicação da Lei Geral de Proteção de Dados.

Com tal disposição normativa, então, a proteção de dados pessoais foi "promovida" a condição de direito fundamental, reforçando a liberdade e a privacidade de todos os cidadãos.

A fim de auxiliar as empresas neste processo de adequação à LGPD, a Federação das Indústrias do Estado do Rio Grande do Sul - FIERGS, e o Centro das Indústrias do Estado do Rio Grande do Sul, CIERGS, elaboraram esta Cartilha sobre **Proteção de Dados Pessoais**, de forma objetiva e simplificada, apresentando diretrizes a serem seguidas para uma eficaz implementação da LGPD nas empresas, a qual será atualizada a cada passo, sendo esta a sua 3ª Edição.

2. De que trata a LGPD?

A LGPD dispõe sobre o tratamento de dados pessoais, em meio físico e em meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ou seja, a LGPD, como **norma de proteção de dados pessoais**, tem por objetivo a proteção do indivíduo (titular das informações).

3. Quais são esses dados pessoais?

Todos os dados que levam à identificação de uma pessoa natural, direta ou indiretamente, identificada ou identificável, 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. Também aqueles que foram descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para identificar uma pessoa.

Na prática, não há distinção entre dados dispostos em meio físico - como documentos impressos - ou em meio digital - como certificados online. Portanto, independentemente do suporte, se houver identificação da pessoa natural, é considerado dado pessoal.

Vejamos abaixo alguns conceitos da Lei:
I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável. Por exemplo: data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos de consumo, entre outros;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter

religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado à uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

IMPORTANTE:
Dados relacionados à titularidade da pessoa jurídica não estão no escopo da lei, ou seja, a LGPD é inaplicável para proteção dos dados de pessoa jurídica.

4. Como devo cuidar esses dados pessoais?

A própria lei conceitua como deve ser realizado o tratamento de dados, que inclui os cuidados que devem ser adotados desde a coleta até a eliminação, ou seja, qualquer ação realizada com os dados pelo controlador é caracterizada como tratamento.

Tratamento, conforme a lei (art. 5º, X), compreende toda a operação realizada com dados pessoais, como as que se referem 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.

Importante destacar que, para a realização de tratamento de dados pessoais, é indispensável que a empresa enquadre cada tratamento realizado em ao menos uma das bases legais exigidas pela lei.

Pela regra, partindo de uma premissa de segurança e boas práticas, as empresas devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Os dados pessoais sensíveis somente devem ser tratados quando o titular ou responsável legal consentir, de forma específica e destacada, para finalidades específicas, ou, sem o consentimento, quando for indispensável o seu tratamento para:

a. cumprimento de obrigação legal ou regulatória pelo controlador;
b. tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
c. realização de estudos por órgão de pesquisa, garantida, sempre que possível, que os dados pessoais permaneçam anônimos;
d. exercício regular de direitos;
e. proteção da vida ou da incolumidade física do Titular ou de terceiros;
f. tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; e
g. garantia da prevenção à fraude e à segurança do Titular.

5. A quem se aplica a LGPD?

A Lei é aplicável a **qualquer** operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio (físico ou digital), do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento de dados ou sua coleta tenham sido realizadas no território nacional ou de indivíduos localizados no território nacional.

Ou seja, as empresas devem se adequar à lei se, por exemplo: coletam dados de clientes para envio de ações promocionais ou de negócios; ou, coletam dados através de site e aplicativos para vender produtos ou serviços; ou analisam comportamento dos clientes para sugerir conteúdo específico; ou,

mantêm dados de colaboradores e utilizam para pagamentos de salários, ou terceirizam a coleta, armazenamento e/ou tratamento de dados pessoais.

A LGPD obriga empresas a cumprirem alguns padrões de segurança. O objetivo é prevenir roubos, vazamentos e a coleta ilegal de informações em meios físicos e digitais.

Cabe destacar que a lei não se aplica aos tratamentos de dados realizados:

a. por uma pessoa física, para fins particulares, e não comerciais (por exemplo: coleta de dados pessoais dos integrantes da família para a montagem de uma árvore genealógica);
b. para fins exclusivamente jornalísticos, artísticos e acadêmicos; e
c. pelo Poder Público - no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

6. Quais são os direitos dos titulares dos dados pessoais?

A LGPD prevê um conjunto de direitos aos titulares de dados pessoais, tais como:

a. direito de acesso facilitado aos seus dados pessoais tratados pela organização;
b. direito de obter a correção dos seus dados pessoais, quando incompletos, inexatos ou desatualizados;
c. direito de obter informações sobre o compartilhamento de seus dados pessoais com outras organizações;
d. o direito a eliminação dos dados coletados e guardados; entre outros.

O direito do titular ao acesso facilitado a informações sobre o tratamento dos seus dados pessoais, inclui o conhecimento acerca: (i) da finalidade especifica do tratamento; (ii) da forma e duração do tratamento; (iii) da identificação e

contato do controlador de dados; (iv) do uso compartilhado dos dados; (v) da existência de um operador de dados, e das responsabilidades do controlador e do operador; (vi) do tratamento dos dados pessoais como condição para a fornecimento do produto ou serviço.

O direito de obter a confirmação da existência de tratamento de seus dados pessoais, deve ocorrer: (i) em formato simplificado, caso a confirmação ou o acesso seja providenciado imediatamente; (ii) por meio de declaração clara e completa, com indicação da origem dos dados (ou inexistência de registro), critérios utilizados e finalidades do tratamento.

Caso a organização tenha compartilhado dados pessoais cuja correção, anonimização, bloqueio ou eliminação fora requerida pelo titular, o pedido deve ser encaminhado à organização que recebeu o compartilhamento, para que também atenda ao requerimento do titular.

Caso o requerimento acerca de um direito do titular de dados não possa ser atendido imediatamente, o controlador deve informar ao titular sobre as razões de fato ou de direito que impedem a adoção imediata de providências, ou comunicar que, na hipótese, não é agente de tratamento.

7. Quais são as hipóteses para o tratamento de dados pessoais?

A Lei também estabelece as hipóteses em que o tratamento de dados pessoais poderá ser realizado, ponto que demanda atenção das organizações. Cabe dizer também que a possibilidade de tratar dados pessoais não se limita ao consentimento do titular.

Vejamos as hipóteses das bases para tratamento de dados expressamente previstas pela legislação:

a. mediante o fornecimento de **consentimento pelo titular**: como por exemplo mediante assinatura de autorização de uso dos dados para participação de um processo seletivo;
b. para o **cumprimento de obrigação legal ou regulatória** pelo controlador: como por exemplo para preenchimento do e-social ou da RAIS;
c. 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 da Lei;
d. para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;
e. 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: como por exemplo para contratação, por parte de um titular de dados, de um serviço cujo objeto principal é o tratamento de dados pessoais, tal como acontece com a inserção de dados em um serviço de armazenamento em nuvem;
f. 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): como por exemplo para uma defesa em um processo administrativo junto ao Ministério Público do Trabalho, ou frente a um Conselho de Classe;
g. para a **proteção da vida** ou da incolumidade física do titular ou de terceiros: como por exemplo no caso de uma pessoa inconsciente dando entrada em um hospital que nunca esteve anteriormente, após sofrer um grave acidente. Nesse caso, o novo hospital precisará de todo o histórico médico do paciente constante, por exemplo, no serviço médico (SESMT) da empresa contratante.
h. para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária: como no exemplo do item anterior, mas aqui os dados serão fornecidos

por outro hospital ou clínica que o paciente costuma frequentar, estando, portanto, autorizado o médico que irá atendê-lo a requisitar a documentação ao outro serviço de saúde, que poderá compartilhar toda a documentação que disponha daquele paciente.

i. quando necessário para **atender aos interesses legítimos** do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais: esta base legal é potencialmente delicada, sendo recomendado utilizá-la somente quando não houver outra base legal aplicável ao caso, pela nebulosidade e fragilidade que envolvem o tema; ou
j. para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente. Para evitar que os titulares de dados pretendessem a sua exclusão, por exemplo, do SPC ou do Serasa, sob a alegação de que não autorizou o respectivo tratamento de dados

8. Como se dá o término do tratamento de dados pessoais?

O término do tratamento dos dados pessoais de um titular, e a sua consequente eliminação da base de dados da organização, ocorrerá quando:

a. a finalidade da coleta foi alcançada, ou na hipótese dos dados não serem mais necessários ou pertinentes para aquela finalidade informada;
b. o titular exercer seu direito de revogação do consentimento (quando essa for a base legal para o tratamento), ou de oposição;
c. pelo decurso do prazo de tratamento, como estabelecido pela organização por determinação da ANPD, quando constatada violação à LGPD.

Entretanto, a LGPD prevê o direito de a organização, mesmo após o término do tratamento, conservar os dados pessoais, nas seguintes hipóteses:

a. para cumprimento de obrigação legal ou regulatória pelo controlador;

b. para fins de estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização.

9. Quem são os agentes da lei? (exemplos)

Titular: pessoa natural a quem se referem os dados pessoais tratados;

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, que pode ser um terceiro;

Encarregado pelo tratamento de dados pessoais: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

As atividades do encarregado consistem em:

a. aceitar reclamações e comunicações dos titulares;
b. prestar esclarecimentos;
c. adotar providências;
d. receber comunicações da autoridade nacional;
e. orientar funcionários e terceiros a respeito das práticas em relação à proteção de dados pessoais;
f. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares que se relacionem a proteção de dados e a privacidade;
g. monitorar as atividades de tratamento de dados.

Autoridade Nacional de Proteção de Dados (ANPD)*: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional;

A ANPD disponibilizou Guia de Agentes de Tratamento, conforme Anexo II.

IMPORTANTE:

- **Controlador** ou **Operador** irão responder pelo dano patrimonial, moral, individual ou coletivo, que vierem a causar em decorrência da violação à legislação de proteção de dados pessoais, cada um por suas ações (art. 42 da Lei).
- **Controladores** atuando em conjunto serão solidariamente responsáveis.
- o **Operador** é solidariamente responsável caso suas atividades sejam contrárias à LGPD ou quando não seguir as instruções do Controlador.

Nenhum dos agentes será responsabilizado, caso não haja violação à LGPD, ou caso o dano seja de culpa exclusiva de terceiros ou do titular dos dados.

10. Quem fiscalizará o cumprimento da lei?

A Autoridade Nacional de Proteção de Dados (ANPD), segundo o art. 5º, XIX e art. 55°-A: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei, bem como aplicar sanções àqueles que descumprirem as normas, entre outros.

A ANPD é composta por: Conselho Diretor (órgão máximo de direção), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas necessárias à aplicação da lei.

* Apenas a ANPD pode isentar empresas da obrigação de constituir um encarregado. Os dados de contato do encarregado deverão ser públicos, permitindo comunicação direta com titulares.

A ANPD regulamentou o Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados por meio da RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 e aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas por meio da RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023, conforme Anexo III.

11. Quais são as sanções previstas na lei?

Os que descumprirem as disposições previstas na LGPD, ficarão sujeitos às seguintes sanções administrativas:

- advertência, com prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento limitada a R$ 50 milhões por infração;
- multa diária, observado o limite mencionado acima;
- publicização da infração;
- bloqueio dos dados pessoais até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções serão aplicadas de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerando sua gravidade e a natureza. Além das sanções administrativas, o infrator poderá responder judicialmente por repercussões decorrentes do descumprimento da LGPD, individual ou coletivamente.

Embora o principal responsável pelos dados seja a empresa, os funcionários que tenham contato com esses dados devem estar atentos à segurança dessas informações, devendo respeitar a política de governança de dados que a empresa adotar.

Importante que as empresas não posterguem suas iniciativas de adequação à LGPD, pois, além das penas administrativas poderá haver judicialização por órgãos como Ministério Público e Procon, assim como por ações diretas de pessoas físicas que de alguma forma possam se sentir lesadas pelo tratamento ilegal de seus dados pessoais

12. O que é um incidente de segurança com dados pessoais?

É um evento que compromete a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

Incidentes podem ocorrer de forma acidental, como o envio de informações para o destinatário incorreto, ou em decorrência de atos intencionais, como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados.

Os incidentes de segurança não se restringem às violações da confidencialidade, abrangem também eventos de perda ou indisponibilidade dados pessoais. São exemplos de incidentes de segurança o sequestro de dados (ransomware), o acesso não autorizado a dados armazenados em sistemas de informação e a publicação não intencional de dados dos titulares.

Nem todo incidente de segurança da informação envolve dados pessoais. Incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificáveis não precisam ser comunicados à ANPD.

A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

Cabe ao Controlador identificar, tratar e avaliar o risco dos incidentes de segurança que afetem suas operações de tratamento de dados pessoais.

13. O que devo fazer em caso de incidente de segurança?

A LGPD impõe aos Controladores, em seu art. 48, o dever de comunicar aos titulares e à ANPD a ocorrência de incidentes que possam causar riscos ou danos relevantes aos titulares. O cumprimento dessa obrigação junto à ANPD e aos titulares afetados, se dá no processo de Comunicação de Incidente de Segurança (CIS).

Portanto, é de extrema importância que todo o colaborador da empresa e/ou organização que identifique um incidente de segurança ou até mesmo esteja em dúvida sobre a natureza do evento, comunique-o imediatamente através do canal adequado, ou seja, aquele disponibilizado pelo Controlador/Operador para o devido reporte, possibilitando assim, que os próximos passos sejam tratados adequadamente pelo Controlador.

A comunicação de incidentes de segurança à ANPD deve ser realizada pelo Encarregado pelo tratamento de dados ou por um representante

legalmente constituído do Controlador, por meio do formulário e orientações, conforme anexo IV.

O formulário deve ser protocolado eletronicamente por meio do Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede).

Para preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, recomenda-se que a comunicação seja feita o mais breve possível, em **até 2 (dois) dias úteis** da ciência do fato.

Após realizada a comunicação, a ANPD verificará a gravidade do fato e determinará as providências que deverão ser adotadas.

- A empresa somente não será responsabilizada quando restar comprovado (Art. 43), que:
  - não realizou o tratamento de dados pessoais que lhe é atribuído;
  - embora tenha realizado o tratamento de dados pessoais, não houve violação à legislação de dados; ou
  - o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

A empresa deve informar ao titular como os dados serão utilizados. Se houver qualquer mudança na finalidade para o tratamento de dados pessoais distintos do consentimento original, a empresa deverá informar previamente o titular dos dados sobre as mudanças de finalidade. Ele poderá revogar o consentimento a qualquer momento, sem custos. Além disso, o titular poderá exigir do controlador, a qualquer momento, confirmação de tratamento de dados, acesso, retificação, cancelamento, oposição, portabilidade, entro outros.

14. O que a minha empresa precisa fazer para estar de acordo com a LGPD?

IMPORTANTE:
Qualquer dado continua podendo ser coletado, mas os dados pessoais devem ser tratados de acordo com a finalidade, ou seja, antes de realizar qualquer procedimento com um dado pessoal, pergunte-se:

POR QUE ESSAS INFORMAÇÕES ESTÃO SENDO MANTIDAS E PROCESSADAS?

Qual é o propósito? Os titulares dos dados pessoais sabem o que é feito com esses dados?

QUE TIPO DE DADO VOCÊ IRÁ COLETAR?

De acordo com a finalidade, você está coletando dados suficientes ou existem dados pessoais irrelevantes que não precisam ser solicitados?

OS DADOS PESSOAIS COLETADOS SÃO REALMENTE NECESSÁRIOS PARA O OBJETIVO FINAL?

É importante que a empresa colete apenas os dados pessoais necessários para aquele fim. Todo e qualquer dado pessoal coletado considerado dispensável/sem finalidade, pode gerar para empresa sanções administrativas.

A finalidade é um dos princípios mais relevantes previstos na lei, o qual preconiza que os dados pessoais deverão ser tratados apenas para as finalidades específicas devidamente informadas aos titulares, e que deve ser observado conjuntamente com o princípio da minimização da coleta, isto é, somente devem ser coletados os dados pessoais mínimos necessários para que se possa atingir a finalidade, e o da retenção mínima, o qual determina a imediata exclusão dos dados, após atingida a finalidade pela qual eles foram coletados – excetuado o caso em que a conservação é necessária para o cumprimento de obrigações legais ou regulatórias, conforme previsto na lei.

Vejamos abaixo o que você precisa fazer diante da coleta de dados:

1. Informar com clareza a finalidade da coleta;
2. Disponibilizar as informações sobre a coleta e o uso desses dados pessoais de forma transparente;
3. Somente poderá manter e utilizar os dados essenciais, o que não for, deverá ser apagado;
4. Se requisitado, a empresa deverá estar preparada para apresentar os dados e a forma como são processadas essas informações;
5. Deve-se manter os dados precisos, removendo ou atualizando os errados ou imprecisos;
6. Informar ao usuário de forma clara e acessível os direitos sobre os seus dados;
7. Deve-se proteger os dados para que não ocorram danos, furtos e/ou perdas, através de medidas de segurança, técnicas e administrativas;
8. Deve-se tomar medidas preventivas de proteção dos dados a fim de evitar danos;
9. Não se deve utilizar os dados para fins discriminatórios, ilícitos ou abusivos;
10. As empresas devem observar os princípios gerais de proteção de dados pessoais previstos na legislação e ter condições de demonstrar isso em todos os procedimentos de gestão adotados.

O processo de adequação exige a adesão da alta gestão da empresa e a criação de um time multidisciplinar, notadamente com a participação de representantes das áreas: jurídica, negócios, tecnologia, recursos humanos, compliance e processos, dentre outros.

Caso a organização/empresa realize o tratamento de grande volume de dados pessoais, sugere-se que o processo de adequação inicie pelas áreas mais impactadas, ou seja, aquelas com capacidade de causar maiores danos aos titulares.

15. Qual passo a passo devo seguir?

De forma ampla, as seguintes etapas constituem sugestões para uma adequação:

1. **ANALISAR DE QUE FORMA A LGPD IMPACTA A EMPRESA:**
   a. Como, por que, e quais categorias de dados pessoais são tratadas pela empresa;
   b. Analisar todo o processo de tratamento de dados pessoais, desde a coleta até o descarte, identificando a finalidade da utilização.
2. **ANALISAR E DOCUMENTAR AS HIPÓTESES LEGAIS PARA O TRATAMENTO DE DADOS, PARA AQUELES SUBMETIDOS À LGPD.**
3. **OBTER OS CONSENTIMENTOS NECESSÁRIOS, SE FOR O CASO.**
4. **REVISAR E DETALHAR A POLÍTICA DE PRIVACIDADE, TORNANDO PÚBLICOS OS SEUS TERMOS AOS INTERESSADOS.**
5. **DEFINIR E DOCUMENTAR AS HIPÓTESES LEGAIS DAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS, SE FOR O CASO.**
6. **ADAPTAR OS CANAIS DE COMUNICAÇÃO, A POLÍTICA E OS PROCESSOS INTERNOS DESTINADOS A ATENDER OS DIREITOS DOS TITULARES.**
7. **DESIGNAR O ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS.**
8. **REVISAR OS ACORDOS E CONTRATOS DA ORGANIZAÇÃO IMPACTADOS PELA LGPD.**
9. **IDENTIFICAR OS POSSÍVEIS RISCOS NO TRATAMENTO DE DADOS E, COMO CONSEQUÊNCIA, PROJETAR E IMPLEMENTAR AS MEDIDAS NECESSÁRIAS PARA GARANTIR A SEGURANÇA DOS DADOS.**
10. **IMPLEMENTAR POLÍTICAS E PROCEDIMENTOS PARA LIDAR COM A OCORRÊNCIA DE EVENTUAIS INCIDENTES.**

Precisa-se mapear os dados que estão sob gestão da sua empresa, sejam eles de clientes, empregados ou prestadores de serviços; entender o que cada setor coleta, revendo as reais necessidades/finalidades; como esses dados são armazenados e descartados, avaliando o chamado de "ciclo de vida" dos dados; de forma a estipular aos responsáveis as regras de operação e gestão dos fluxos dos dados.

Portanto, estar pronto para a LGPD significa que:

- todas as pessoas, de todas as áreas da empresa devem conhecer os princípios, direitos e deveres da lei, afinal todas as áreas utilizam dados de clientes e/ou dos empregados em suas atividades;
- toda empresa deve identificar quais dados pessoais ela utiliza, como gerencia, onde estão, quem os utiliza, qual propósito, como são descartados e como eles são protegidos;
- a empresa deve possuir um canal de suporte às solicitações do titular de dados, ANPD ou outros órgãos fiscalizadores;
- as empresas devem garantir que empresas terceirizadas que tratam dados pessoais sob sua responsabilidade também estejam em conformidade com a LGPD.

16. LGPD e sindicatos

A LGPD se aplica aos Sindicatos, uma vez que estes tratam dados pessoais relativos aos associados, dirigentes, parceiros e empregados.

Os dados são necessários para a representação do segmento, envio de comunicados, convites, informativos, cobranças de anuidade ou mensalidade, bem como outras atividades.

Logo é importante que os sindicatos e associações tenham cuidado com a coleta, processamento e qualquer outro tratamento de dados pessoais não

só de seus associados, mas de todos aqueles com quem se relacionam no exercício de suas atividades.

A LGPD pede cautela e atenção no compartilhamento de dados pessoais com empresas e entidades terceiras, seja por parcerias ou prestação de serviço.

Em várias dessas relações a base legal será o contrato firmado, o vínculo de emprego ou o próprio estatuto da entidade. Mas, em várias relações o consentimento específico para o fim de compartilhamento será peça-chave nestas situações para deixar clara ao titular a finalidade a qual seu dado pessoal se destina.

Importante lembrar que:
Dados pessoais relacionados à filiação a sindicato enquadram-se no conceito de dados pessoais sensíveis. Devido ao seu teor e às consequências negativas e discriminatórias que seu vazamento pode causar ao titular, inclusive gerando direito à reparação moral tanto na esfera trabalhista quanto cível, a lei tratou de defini-los como “sensíveis” e prever tratamento especial, com bases legais inclusive mais restritivas.

Sendo assim, não seria possível, por exemplo, valer-se do legítimo interesse (Base Legal que pode ser aplicada para Dados Pessoais não sensíveis) para criar uma lista com os associados sindicalizados e sua filiação sindical e enviar convites e informações como reuniões, cursos, seminários, pesquisas, moções, buscas e outras formas de interações. Neste caso, a base legal mais apropriada seria a do consentimento, com a devida coleta de autorização, bem como com a opção de saída, a qualquer momento, pelo associado.

Por outro lado, sindicatos e associações podem, a exemplo, utilizar a base legal de exercício regular de direitos e, ainda, de obrigação legal ou regulatória para armazenar a relação dos nomes dos associados sindicalizados e respectivas Guias de Recolhimento de Contribuição Sindical (GRCSU) com

vistas à representação de classe prevista pela Constituição Federal e para eventual salvaguarda quando do ajuizamento de eventual reclamação trabalhista.

Relativamente aos sindicatos e associações, o cuidado com a LGPD está voltado para 3(três) grupos principais: 1) Colaboradores: Presidência, Diretoria, Gestores, Empregados do sindicato; 2) Associados; e 3) Terceiros, de maneira geral: prestadores de serviços, fornecedores, parceiros de negócio e usuários de determinado website ou visitantes nas dependências do sindicato.

Assim, para Colaboradores, os Dados Pessoais poderão ser tratados em decorrência do contrato de emprego firmado, por exemplo, ou para o cumprimento de obrigações legais e regulatórias (exemplo: informações transmitidas ao E-Social) ou, ainda, para permitir o exercício regular de direitos em caso do ajuizamento de reclamações trabalhistas. Para a transparência, recomenda-se a elaboração de um Aviso de Privacidade Interno e Políticas de Privacidade.

Quanto à relação com os Associados, devem receber total transparência a respeito de quais dados pessoais são coletados e tratados. Muitas das atividades sindicais são envios de comunicação, eventos, palestras, clubes de benefícios e a escolha pela adesão deve ser tratada de forma livre pelo Associado, nesses casos, o consentimento também parece ser a melhor opção para tratamento de Dados decorrentes de tais atividades.

Por fim, a relação com Terceiros, no caso em que houver o compartilhamento e tratamento de dados pessoais entre as Partes, os contratos devem conter cláusulas específicas para que se estabeleça os critérios e padrões mínimos para condução do tratamento e definição das responsabilidades entre os agentes. Para a transparência, recomenda-se também a elaboração de um Aviso de Privacidade Externo.

Importante ter presente que todo e qualquer tratamento envolvendo dados pessoais deve estar amparado por uma base legal, ciente de que, o consentimento é a única base legal que pode ser revogada a qualquer momento. Logo, caso o titular revogue o consentimento, deve-se analisar se, (1) - atingida a finalidade pretendida com o tratamento daquele dado pessoal (o que, em tese, gera a obrigação de não mais utilização) ou (2) - se solicitada a exclusão, por exemplo, pelo titular, há alguma outra base legal que ampare a continuidade desse tratamento; ou, (3) - caso negativo, se é possível a anonimização desses dados pessoais. Se frustrada as etapas acima, a revogação deve ser concedida ao titular.

17. LGPD nas pequenas empresas e startups

Conforme determina expressamente a legislação, a ANPD regulamenta a aplicação da LGPD para os agentes de pequeno porte. Tal cumprimento foi cumprido com a publicação da Resolução CD/ANPD nº 2 (Anexo V).

Segundo a regulamentação, são considerados agentes de pequeno porte:

- Microempresas;
- Empresas de pequeno porte;
- Startups;
- Pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação;

São pequenas empresas as entidades com faturamento anual de até R$ 4,8 milhões e até 99 funcionários. A microempresa poderá ter faturamento anual de até R$ 360 mil e 19 funcionários, enquanto o microempreendedor individual poderá ter faturamento anual máximo de R$ 81 mil e 1 funcionário.

Já as startups, são definidas como: (i) empresas com até 10 anos de inscrição no cadastro nacional de pessoa jurídica (CNPJ); (ii) com faturamento bruto

anual máximo de R$ 16 milhões; e (iii) que utilizem modelos de negócios inovadores para geração de produtos ou serviços.

- Não estão amparados por esta norma, os agentes de tratamento de pequeno porte que realizem tratamento de alto risco, atendendo cumulativamente a pelo menos um critério geral e um critério específico, conforme abaixo:
  I. critérios gerais:
     a. tratamento de dados pessoais em larga escala; ou
     b. tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
  II. critérios específicos:
     a. uso de tecnologias emergentes ou inovadoras;
     b. vigilância ou controle de zonas acessíveis ao público;
     c. decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
     d. utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

O que muda para essas empresas que se enquadram nestas exceções?

Registro das Atividades de Tratamento

A obrigação de elaboração e manutenção dos registros das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, poderá ser feita de forma simplificada, sendo fornecido pela ANPD modelo para este registro, conforme anexo VII;

Comunicações dos Incidentes de Segurança

A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança.

Encarregado pelo Tratamento de Dados Pessoais

Os agentes de pequeno porte não serão obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD, porém, deverão disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.

Se houver indicação de encarregado, será considerada como política de boas práticas e governança, podendo atenuar eventual aplicação de sanções pela ANPD.

Segurança e das Boas Práticas

Devem ser adotadas medidas administrativas e técnicas, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais. No entanto, essas empresas podem estabelecer uma política simplificada de segurança da informação, desde que garanta a proteção contra situações acidentais ou ilícitas, tais como alteração de dados, destruição, perda, entre outros.

Prazos Diferenciados

Será concedido **prazo em dobro** nas seguintes situações:

- No atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais;
- Na comunicação à ANPD e ao titular da ocorrência de incidente de segurança, exceto quando houver risco à integridade física ou moral dos titulares ou à segurança nacional;
- No fornecimento de declaração clara e completa de confirmação de existência ou de acesso a dados pessoais;
- No fornecimento de declaração simplificada de existência ou de acesso a dados pessoais em formato simplificado, que trata o art. 19, I, da LGPD, em até 15 dias, a partir do requerimento do titular;

- Na apresentação de informações, documentos, relatórios e registros solicitados pela ANPD.

Importante destacar que a dispensa ou flexibilização das obrigações dispostas não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD.

Perguntas e Respostas

1. Qual é o objetivo da LGPD e a quem ela se destina?

A LGPD foi criada com o objetivo de proporcionar ao cidadão brasileiro um controle maior sobre o tratamento de seus dados pessoais. Para isso, a LGPD estabelece princípios e cria regras que devem ser observados tanto por organizações privadas quanto públicas, além de criar entidade reguladora específica para o tema.

2. Quem fiscaliza o cumprimento da lei?

A fiscalização referente à LGPD será primariamente realizada pela Autoridade Nacional de Proteção de Dados (ANPD). Este órgão foi criado para fiscalizar o cumprimento da lei, zelar pela proteção de dados pessoais, elaborar diretrizes e também aplicar as sanções em casos de irregularidade. Além disso, a ANPD guiará a interpretação da Lei e regulamentará padrões e técnicas aplicáveis às questões de segurança da informação, interoperabilidade e processos de anonimização, além de poder requisitar informações sobre tratamentos de dados pessoais para agentes de tratamento, editar normas e orientações.

Destacamos que o Ministério Público continua competente para lidar com a questão no que tange os direitos difusos dos cidadãos e direitos individuais dos consumidores.

3. Quem é o “titular”?

É a pessoa natural a quem se referem os dados pessoais que são objetos de coleta e tratamento.

4. O que são “dados pessoais”?

De acordo com a lei, um dado pessoal é informação relacionada à pessoa natural identificada ou identificável. Como exemplos: nome, número do CPF, data de nascimento, endereço residencial e e-mail.

5. O que são “dados pessoais sensíveis”?

É qualquer dado pessoal, conforme estabelecido na lei, 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.

6. O que compreende o tratamento destes dados?

O tratamento de dados é um conceito abrangente, que inclui qualquer tipo de manipulação realizada com informações pessoais. Processos comuns a diversos tipos de empresas incluem, geralmente, a coleta, a reprodução, o acesso, o armazenamento e a distribuição de dados pessoais. Um exemplo simples: A criação de uma lista de e-mails.

7. Em quais casos de tratamento de dados pessoais a lei é aplicada?

A lei se aplica a qualquer operação que envolve a coleta e o tratamento de dados pessoais e que seja realizada em território brasileiro.

8. Esta Lei aplica-se apenas ao tratamento de dados pessoais coletados na Internet?

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais que tenham sido coletados dentro do território brasileiro ou que tenha como objetivo oferecer bens ou serviços a pessoas localizadas no Brasil,

independentemente destes dados pessoais terem sido coletados offline ou online, em meios físicos ou digitais.

9. Mas o que são dados pessoais coletados offline ou online?

Dados pessoais coletados offline são obtidos sem a utilização de ferramentas informatizadas, como por exemplo, a lista de presença em eventos.

Os dados pessoais coletados online são os que utilizam ferramentas informatizadas e/ou automatizados para serem obtidos, tais como os cadastros de candidatos para vagas de emprego.

10. Quais são os principais atores no tratamento de dados pessoais de acordo com a LGPD?

São três: o Controlador, o Operador e o Encarregado.

O **Controlador** é pessoa natural ou jurídica de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

O **Operador** é pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O **Encarregado** é a pessoa indicada pelo controlador e/ou operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

11. Quais são os casos de tratamento de dados pessoais em que a LGPD não será aplicada?

São os casos em que o tratamento de dados pessoais for feito por uma pessoa física, para fins particulares, e não comerciais, por exemplo, coleta de dados pessoais dos integrantes da família para a montagem de uma árvore genealógica; para fins exclusivamente jornalísticos, artísticos e acadêmicos; ou pelo Poder Público - no caso de segurança pública, defesa nacional, segurança

do Estado e atividades de investigação e repressão de infrações penais.

12. O que é um dado anônimo ou anonimizado?

Dado anônimo ou anonimizado é qualquer dado pessoal que, submetido a meios técnicos razoáveis, passe a não mais identificar ou a proporcionar a identificação de uma pessoa natural, direta ou indiretamente, de maneira definitiva e irreversível.

13. O tratamento de dados pessoais sensíveis pode ser realizado em quais condições?

O tratamento de dados pessoais sensíveis somente poderá ocorrer com consentimento do titular ou seu responsável legal, de forma destacada e para finalidades específicas.

Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

I. cumprimento de obrigação legal ou regulatória pelo controlador;
II. pela administração pública, de políticas públicas previstas em leis ou regulamentos;
III. estudos por órgão de pesquisa;
IV. exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
V. proteção da vida;
VI. tutela da saúde;
VII. garantia da prevenção à fraude e à segurança do titular.

14. Se a empresa for sediada no exterior, também tem deve se adequar à Lei?

Caso a empresa ofereça bens ou serviços para pessoas localizadas no Brasil e, portanto, coletar dados de usuários, a LGPD também se aplica e com isso a empresa deve se adequar.

15. Quais são os princípios da LGPD?

A LGPD traz alguns princípios que devem ser respeitados no tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

16. Quais são as Bases Legais para tratamento de dados pessoais?

O tratamento de dados pessoais somente poderá ser realizado:

- Com consentimento do titular;
- Para cumprimento de obrigação legal ou regulatória;
- Pela Administração Pública;
- Para realização de estudos por órgãos de pesquisa;
- Para execução de contratos, a pedido do titular;
- Para exercício de direitos em processos judiciais, administrativos ou arbitrais;
- Para proteção da vida;
- Para tutela da saúde;
- Em legítimo interesse do Controlador;
- Para proteção do crédito.

17. O que é “consentimento”?

É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento e sua finalidade devem estar claros e destacados.

18. E quando a finalidade muda, o que a empresa deve fazer?

Se a empresa precisa de um dado pessoal já coletado com o consentimento do titular para outra finalidade de uso, é necessário informá-lo sobre este novo intuito. Importante ressaltar que, além de informar é preciso atualizar o consentimento do titular.

19. O termo de consentimento deve ser escrito ou digital?

O termo de consentimento, como consta no Art. 8, pode ser adquirido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

20. O titular dos dados pode revogar seu consentimento?

Sim, a LGPD estabelece que o titular dos dados poderá, a qualquer momento, revogar seu consentimento.

21. Há alguma diferença entre o consentimento para o tratamento de dados pessoais e para tratamento dados pessoais sensíveis?

Não. O consentimento para dados sensíveis deve sempre explicitar a finalidade de seu uso, de forma destacada. Se houver alteração na finalidade, é preciso renovar o consentimento de forma expressa.

22. Como se dá o consentimento de Crianças e Adolescentes?

A LGPD estabelece, no artigo 14, que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse. Para tratamento de dados de crianças até 12 anos de idade é necessário consentimento específico e em destaque, dado por, pelo menos, um dos pais ou pelo responsável legal.

Os dados de crianças e adolescentes poderão ser coletados sem o consentimento, quando for necessário para sua proteção ou para contatar os pais ou o responsável legal, sendo utilizados uma única vez e sem armazenamento. Os dados de menores não poderão ser repassados a terceiros sem o expresso consentimento para tal.

23. Quando o interesse é considerado legítimo?

Conforme o Guia Orientativo das Hipóteses Legais de Tratamento de Dados - Legítimo Interesse, lançado pela Autoridade Nacional de Proteção de Dados (ANPD), o interesse será considerado legítimo quando atender três condições:

(i) compatibilidade com o ordenamento jurídico; (ii) lastro em situações concretas; e (iii) vinculação a finalidades legítimas, específicas e explícitas.

A compatibilidade com o ordenamento jurídico pressupõe que o interesse esteja em conformidade com princípios, normas jurídicas e direitos fundamentais. O lastro em situações concretas, significa hipóteses reais, claras e precisas, que objetivem interesses específicos e bem delineados, o que afasta interesses considerados a partir de situações abstratas ou especulativas. E a terceira condição a ser demonstrada é o propósito específico que se pretende alcançar com a realização do tratamento, que deve ser considerado a partir de situações concretas, com o uso de dados pessoais estritamente necessários para a finalidade pretendida.

24. Em casos de irregularidade no tratamento de dados, quem será responsabilizado?

Se o tratamento de dados não acontecer como previsto na lei, os Controladores serão responsabilizados. Caso o Operador não tenha cumprido ordens passadas pelo Controlador ou ocorra falha na segurança dos dados, este também pode ser penalizado.

25. Quais são as penalidades que podem ser aplicadas nos casos de irregularidades?

A penalidade imposta irá depender da avaliação da ANPD, mas pode ser uma advertência, a determinação da publicação e divulgação da infração cometida, o bloqueio ou eliminação dos dados que sofreram violações e também multas simples e/ou diárias.

26. Ações que infrinjam a lei podem acarretar em imposição de multas?

As multas são de até 2% do faturamento da empresa, limitados a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, além da possibilidade de suspensão das atividades de coleta e tratamento, sem prejuízo da indenização pelos danos que causarem aos titulares dos dados.

27. O que é GDPR?

A General Data Protection Regulation (GDPR) é a Lei europeia vigente que trata da proteção de dados pessoais, que inspirou a elaboração. As empresas e órgãos estatais brasileiros que mantenham negócios com os países europeus terão a obrigatoriedade de garantir que suas políticas de tratamento de dados estejam em conformidade com a GDPR, sob o risco de penalidades, bem como perda de clientela, valor de marca e credibilidade no mercado internacional.

28. O que é DPO?

DPO, ou Data Protection Officer, é o encarregado que irá atuar como canal de comunicação entre o Controlador, os titulares dos dados e a ANPD.

A ANPD lançou em Dezembro/2024 o Guia Orientativo Atuação do Encarregado pelo Tratamento de Dados Pessoais. Para compreender a atuação do DPO acesse Anexo XI.

29. O que são cookies ?

Cookies são pequenos arquivos de texto que contém várias informações sobre os visitantes de um website. A principal função de um cookie é identificar e armazenar informações desses usuários. Um website pode utilizar diversos cookies para as mais variadas necessidades. Eles podem armazenar informações como nome, e-mail, IP e páginas visitadas, e são utilizados como recurso técnico para manter, por exemplo, a sessão de preferencias dos usuários de maneira correta, ou para fins de estatísticas e marketing. Fonte (Guia Prático de Implementação da LGPD – Daniel Donda, Editora Labrador).

A ANPD lançou em Outubro/2022 o Guia Orientativo Cookies e proteção de dados pessoais, cuja leitura se recomenda.

30. O Poder Público também está sujeito às disposições da LGPD?

Sim, os dados pessoais tratados pelo Poder Público também estarão sujeitos à LGPD. Porém, o Poder Público pode tratar dados pessoais sem pedir o

consentimento do titular sempre que for necessário para a execução de políticas públicas. O Poder Público também poderá tratar dados pessoais, fora do escopo da lei, no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, que serão tratados de acordo com legislação específica, que contenha medidas proporcionais e necessárias para que o tratamento de dados pessoais atenda ao interesse público. Para a criação das normas específicas para esses casos, a Autoridade Nacional de Proteção de Dados Pessoais - ANPD emitirá recomendações e opiniões técnicas.

31. É possível o uso compartilhado de dados entre diferentes órgãos da Administração Pública?

A Lei permite o uso compartilhado de dados pessoais entre entes do poder público, desde que atenda a finalidades específicas de execução de políticas públicas e a atribuição legal desses órgãos, respeitados os princípios do art. 6º. O inciso III do art. 7º assegura, como uma de suas dez bases legais para o tratamento de dados, o tratamento e uso compartilhado pela Administração Pública de dados necessários à execução de políticas públicas previstas em leis, regulamentos ou ainda respaldadas em contratos, convênios ou instrumentos congêneres, nos termos do Capítulo IV.

32. A LGPD dispõe sobre a transferência de dados entre o Poder Público e instituições do setor privado?

O artigo 26 prevê que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei.

Veta a transferência dos dados pessoais constantes de bases de dados a que tenha acesso, exceto:

Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

Em casos em que os dados forem acessíveis publicamente;

Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

Para prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados.

33. Em que casos os dados pessoais podem ser transferidos para fora do Brasil?

A transferência internacional de dados pessoais pode ser feita:

I. Para países ou organizações internacionais proporcionem grau adequado de proteção de dados pessoais;
II. Quando o Controlador oferecer e comprovar, por meio de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados ou códigos de conduta regularmente emitidos, que está cumprindo com o disposto na LGPD;
III. Quando necessário para cumprimento de acordos da cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e persecução, de acordo com os instrumentos de direito internacional;
IV. Para proteção da vida do titular ou de terceiros;
V. Quando autorizada pela ANPD;
VI. Quando resultar em compromisso assumido em acordo de cooperação internacional;
VII. Para a execução de política pública;

VIII. Quando o titular fornecer seu consentimento de forma específica e em destaque para a transferência;
IX. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
X. Quando necessário para a execução de contrato do qual seja parte o titular;
XI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Para compreender sobre a transferência internacional de dados acesse o Anexo X.

34. Em caso de incidente o titular deverá ser informado?

A LGPD determina que o Controlador deverá comunicar tanto ao titular quanto à ANPD sobre a ocorrência de qualquer incidente de segurança que possa causar risco ou dano ao titular.

35. Como a LGPD protege os titulares de decisões automatizadas, baseadas exclusivamente em meios tecnológicos?

O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Além disso, o Controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

36. É necessário adequar o tratamento dos dados de Pessoas Jurídicas na base de clientes da empresa?

É necessário adequar o tratamento dos dados dos clientes que correspondam a pessoas naturais vinculadas ao cadastro da Pessoa Jurídica, pois a LGPD

regulamenta apenas o tratamento de dados pessoais.

37. Qual o papel da tecnologia na implementação da LGPD?

A análise e as ações para entrar em conformidade com a LGPD devem passar por pessoas, processos e tecnologia. Por conta de todas as variáveis envolvidas, o uso da tecnologia faz muita diferença e é importante, pois, dependendo do tamanho e nível de complexidade de uma organização, gerenciar todo o ambiente de acordo com os requisitos da lei sem uma ferramenta de gestão que consiga agregar, registrar e controlar todas as demandas pode se tornar extremamente difícil.

Segundo o Art. 49 da Lei, 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 Lei e às demais normas regulamentares.

38. O que é compartilhamento de dados pessoais?

De acordo com a lei é considerado compartilhamento de dados toda 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.

39. Como é permitido o compartilhamento de dados pessoais?

De acordo com a LGPD, o compartilhamento de dados pessoais pode ocorrer em caso de consentimento expresso e específico do titular dos dados e 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.

40. É permitido o compartilhamento de dados pessoais sensíveis?

A LGPD já determina que o compartilhamento de dados sensíveis com o objetivo de obter vantagem econômica poderá ser vedado ou regulamentado pelas autoridades, e no caso específico de dados de saúde determina a vedação, exceto nos em casos de consentimento expresso ou para a adequada prestação de serviços de saúde suplementar, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia.

41. A LGPD restringe a tomada de decisões automatizadas baseadas no uso de algoritmos?

O uso de algoritmos não é vedado pela LGPD. No entanto, o artigo 20, que aborda decisões tomadas exclusivamente por meio de automação, ou seja, sem participação de seres humanos, determina que o titular dos dados pode, sempre que desejar, requerer a revisão de decisão automatizada que afete seus interesses.

42. Como fica o relacionamento com parceiros comerciais?

Será necessária revisão dos contratos e procedimentos, com a inclusão de cláusulas específicas sobre proteção de dados com clientes e fornecedores em que possa ocorrer o compartilhamento de dados pessoais de terceiros. Será necessária também a adoção de procedimentos e ferramentas capazes de certificar a segurança dos dados compartilhados.

43. Como proceder em caso de incidente de segurança com dados pessoais?

Além de executar as medidas para reverter ou mitigar os efeitos do incidente, conforme plano previamente estabelecido de resposta a incidentes e remediação da empresa, a LGPD impõe aos controladores, em seu art. 48, o dever de comunicar aos titulares e à ANPD a ocorrência de incidentes que possam causar riscos ou danos relevantes aos titulares. O cumprimento dessa obrigação junto à ANPD e aos titulares afetados, se dá no processo de Comunicação de Incidente de Segurança (CIS).

Para comunicar a ANPD, siga as orientações, conforme Anexo IV.

44. Quais incidentes de segurança precisam ser comunicados aos titulares e à ANPD?

Somente os controladores sujeitos à Lei Geral de Proteção de Dados têm obrigação de comunicar os incidentes à ANPD.

Um incidente precisa ser comunicado se atender, cumulativamente, aos seguintes critérios:

1. Tenha a ocorrência confirmada pelo agente.
2. Envolva dados pessoais sujeitos à LGPD.
3. Acarrete risco ou dano relevante aos titulares dos dados.

Veja exemplos de incidentes capazes de gerar risco ou dano relevante aos titulares:

A invasão de uma rede de computadores de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais.

A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados, impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde.

A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

45. A adequação à lei difere por ramos de atividade? Existem disposições específicas em relação aos sindicatos e associações?

Todos estão sob a égide da LGPD. Para regulamentar disposição legal específica, a ANPD publicou recentemente texto legislativo específico para flexibilizar as exigências às empresas de pequeno porte e startups.

Para compreender sobre a adequação de empresas de pequeno porte, acesse o Anexo V.

46. Quais empresas são obrigadas a se adequar?

Todas as empresas e/ou pessoas físicas que realizem o tratamento de dados para fins econômicos estão sujeitas a LGPD.

47. Dentro da empresa, quais setores serão mais impactados? Comercial, financeiro, RH, jurídico?

Todos os setores que lidam com dados de clientes e/ou empregados (pessoa física), serão impactados.

48. É necessário o consentimento do titular dos dados para enviar informações ao eSocial?

Não é necessário o consentimento do titular, pois o eSocial exige o envio dos dados cadastrais do funcionário. A Empresa deve manter processos de segurança para a salvaguarda dos dados dos empregados.

49. Qual é o prazo para as Empresas se adequarem a LGPD?

A lei já está em vigor. As Empresas devem se adaptar aos Artigos da Lei o quanto antes. Os titulares dos dados já podem relatar incidentes ligados ao uso indevido dos seus dados, perante o Encarregado da Organização, ANPD ou ainda, junto aos órgãos de defesa dos consumidores.

Referências

ANEXO I - Lei Nº 13.709, de 14 de agosto de 2018
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

ANEXO II - AGENTE DE TRATAMENTO

ANEXO III - Quem Fiscalizará o Cumprimento da Lei
RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023 - Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

ANEXO IV - O que devo fazer em Caso de Incidente de Segurança com Dados Pessoais
https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd#:~:text=O%20Peticionamento%20Eletr%C3%B4nico%20possibilita%20a,em%20formato%20f%C3%ADsico%20ao%20Protocolo

ANEXO V - Agente de Tratamento de Pequeno Porte
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte

Checklist alinhado - vf (www.gov.br)

https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

ANEXO VI – Proteção de Dados como Direito Fundamental

ANEXO VII – Registro das Operações de Tratamento de Dados Pessoais
Formulário Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP): versão excel; versão pdf.

ANEXO VIII – Guia Orientativo – Cookies e Proteção de Dados Pessoais

ANEXO IX – Guia Orientativo - Hipóteses Legais de Tratamento de Dados Pessoais - Legítimo Interesse

ANEXO X – Regulamento Sobre a Transferência Internacional de Dados
https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396

https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/assuntos-internacionais-pt

ANEXO XI – Guia Orientativo – Atuação do Encarregado pelo Tratamento de Dados Pessoais

Federação das Indústrias do Estado do Rio Grande do Sul

Gestão 2024 - 2027
PRESIDENTE
Claudio Affonso Amoretti Bier

FIERGS

VICE-PRESIDENTES:
André Bier Gerdau Johannpeter
Arildo Bennech Oliveira
Claudio Teitelbaum
Clovis Tramontina
Maristela Cusin Longhi
Ubiratã Rezler

DIRETORES:
Airton Capoani
Alexandre de Andrade Isoppo
Antonio Candido Prataviera Calcagnotto
Argileu de Souza Barboza
Betuel Brun Sauer
Carlos Weinschenck de Faria
Carolina Luisa Rossato
Cesar Augusto Carlotto
Claudino João José Simon
Cristiano Basso
Delorges Antônio Horta Duarte
Eduardo Rodrigues de Freitas Machado
Enio Garcia
Ervino Ivo Renner
Flávia Regina Matzenbacher
Gilberto Pedrucci
Giuliano Fornazier
Guilherme Portella dos Santos
Hernane Kaminski Cauduro
Irineu Boff
Jairo Luis Valandro
Juarez José Piva
Leo Clóvis Fabris
Leonardo Souza De Zorzi
Luiz Felipe Schiavon
Luis Felipe Walter
Maria Ines Menegotto de Campos
Nerison Antonio Paveglio
Paulo Fernando Rosa Paim
Rafael Gustavo Araujo Ribeiro
Rafael Sacchi
Roberto Rene Machemer
Rodrigo Cesar Koebe Weissheimer
Rogério Klebanowski Milagre
Samir Frazzon Samara
Torquato Ribeiro Pontes Netto
Valmor Thesing
Walter Rudi Christmann

CONSELHO FISCAL:
Airton Zoch Viñas
Rodrigo Holler Petry
Roque Noschang
Carlos Lazzari
Gilberto Luiz Bortoluzzi
Valterez Ferreira da Silva

DELEGADOS REPRESENTANTES JUNTO À CNI:
Claudio Affonso Amoretti Bier
Gilberto Porcello Petry
Daniel Raul Randon
José Antonio Fernandes Martins

Centro das Indústrias do Estado do Rio Grande do Sul

Gestão 2024 - 2027
PRESIDENTE
Claudio Affonso Amoretti Bier

CIERGS

VICE-PRESIDENTES:
Alexandre Guerra
Erasmo Carlos Battistella
Gilberto Ribeiro
Julio Ricardo Andrighetto Mottin
Mauro Gilberto Bellini
Ricardo Lins Portella Nunes

VICE-PRESIDENTES REGIONAIS:
Angelo Cesar Fontana
Aquiles Dal Molin Junior
Geraldo José Alexandrini
Irani Tadeu Cioccari
Jairo Alberto Zandoná
Júlio Carlos Cardoso Kirchhof
Luiz Roberto Saalfeld
Otto Trost
Ruben Antonio Bisi
Tibúrcio Aristeu Grings

DIRETORES:
Ademar De Gasperi
Aderbal Fernandes Lima
Alexandre Bittencourt De Carli
Aline Eggers Bagatini
Anderson Pontalti
Antonio Lacerda
Bernardo Bregoli Soares
Celso Theisen
Cláudio Guenther
Daniel Martin Ely
Daniela Aesse Kraemer
Diogo Paz Bier
Élio Jorge Coradini Filho
Fernando José Ruschel Justo
Gerenise Viezzer
Gilberto Antônio Piccinini
Guilherme Scozziero Neto
Gustavo Souto Polese
Joarez José Piccinini
José Luis Korman Tenenbaum
Julio Ricardo Mottin Neto
Leonardo Botelho Zilio
Luciano André Merigo
Marcelo Luís Wallauer
Marcus Coester
Mathias Elter
Paulo Roberto Sachett
Rafael Goellner Garcia
René Ormazabal Moura
Reomar Angelo Slaviero
Ricardo Escoboza
Rodrigo dos Santos Fantinel
Walter Rauen de Souza

CONSELHO FISCAL:
Adair Angelo Niquetti
Carla Carnevali Gomes
Jorge Romeu Ritter
Eduardo Lima Cervelin
Ricardo Dias Michelon
Viviane Robinson Martinez

COORDENADOR DO CONSELHO DE RELAÇÕES DO TRABALHO (CONTRAB)
Guilherme Scozziero Neto

VICE-COORDENADOR
Eduardo Lima Cervelin

CONSELHEIROS DO CONTRAB:
Airton Capoani
Alessandra Lucchese
Alexandre Capitanio Michelin
Alfeu Muratt
Ana Cristina Marques Cardoso Quevedo
André Renato Zuco
Antonino Germano
Arthur Giovanardi Dozza
Benôni Canellas Rossi
Bruno Milano Tricerri
Cleber de Assunção e Silva
Diego Martignoni
Edson Morais Garcez
Eduardo Caringi Raupp
Eliana Fialho Herzog
Eugênio Hainzenreder Júnior
Felipe Ziegler Zugno
Fernando Gonçalves Amaral
Fernando Kerber
Gabriela Rita Santurio Pisorno
Giovane Motta de Castro
Gisele de Morais Garcez
Gisele de Morais Garcez
Gustavo Juchem
Gustavo Vielmo Corrêa
Hevelisa de Assis Medeiros
Jacinta Sidegum Renner
João Vicente Rothfuchs
José Paulo Boelter
José Pedro Pedrassani
Julia Cigana Schenkel
Julio Carlos Cardoso Kirchhof
Leandro Custódio
Luciano Benetti Correa da Silva
Luciano da Cas Sima
Luciano Valasqui
Luiz Arthur Pacheco de Castro
Luiz Fernando Souza dos Santos
Maiara Cristina Gaio
Marcelo Ayub
Marcelo Pascotini
Márcia Helena Somensi
Marcio Rogério Basotti
Marco Antônio de Lima
Marcos Giovane Rutsatz
Patrícia Cardoso Rosa
Patricia Manica
Paulo Roberto Tramontini
Ranniery Camara Castello
Renan Schwengber
Renata Kerkhoff
Ricardo Abel Guarnieri
Ricardo Dias Michelon
Roberto Pierre Bersch
Rogério Luiz Balbinot
Rosangela Benetti Almeida
Sergio Armando de Almeida Weltere
Sérgio Luiz de Macedo Ussan
Thiago Guedes
Vanessa Tissiani Borges Gasparin
Vitor Hugo Facchin

COORDENADORA DO GRUPO DE ESTUDOS SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS
Ana Cristina Quevedo

VICE-COORDENADORA
Eliana Herzog

CONSELHEIROS:
Ana Caroline Braun
Bruno Milano Tricerri
Carlos Moeller
Debora Cristiane Dullius
Fabio Cesar Müller Vieira
Felipe Ziegler Zugno
Gabriela Guimarães Müller
Martha Leal
Renata Kerkhoff
Rogineli Prigol
Rosangela Benetti Almeida
Suelen da Silva Rocha
Vanessa Nascimento Cardoso

COORDENADOR GERAL DA GETEC
Clovis Tramontina

DIRETOR EXECUTIVO DO SISTEMA FIERGS - CIERGS
Paulo Renato Hermann

DIRETORA DE RELAÇÕES INSTITUCIONAIS
Ana Paula Werlang

GERÊNCIA TÉCNICA DE APOIO AOS CONSELHOS TEMÁTICOS (GETEC)
Luciano D'Andrea

EQUIPE EXECUTIVA DO CONTRAB:
Fabio Cesar Müller Vieira
Franklin Morais dos Santos
Gabriela Guimarães Müller
Suelen da Silva Rocha

DÚVIDAS E INFORMAÇÕES

entre em contato conosco pelo
e-mail contrab@fiergs.org.br
ou pelo telefone (51) 3347-8632.

Sistema

FIERGS

SESI | SENAI | IEL | CIERGS