CARTILHA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

OAB MINAS GERAIS

INOVAR, INCLUIR E AVANÇAR

CARTILHA SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Presidente:
SÉRGIO RODRIGUES LEONARDO

Vice-Presidente:
ANGELA PARREIRA DE OLIVEIRA BOTELHO

Secretário Geral:
SANDERS ALVES AUGUSTO

Secretário Geral Adjunto:
CASSIA MARIZE HATEM GUIMARAES

Tesoureiro:
FABRICIO SOUZA CRUZ ALMEIDA

Tesoureiro Adjunto:
MARCO ANTONIO OLIVEIRA FREITAS

Diretor Institucional:
ROMULO BRASIL DE AVELAR CAMPOS
WAGNER ANTONIO POLICENI PARROT

Diretor de Apoio as Subseções:
ALVARO GUILHERME RIBEIRO MATOS

Diretor de Prerrogativas:
ERCIO QUARESMA FIRPE

Diretor de Interiorização:
BERNARDO CARVALHO BRANT MAIA
MARCIO FACCHINI GARCIA
RODRIGO CARVALHO FERNANDES MARTINS RIBEIRO

Diretor de Inclusão:
WILLIAM DOS SANTOS

Presidente da Comissão Proteção de Dados:
Melissa Barrioni

Vice Presidente da Comissão de Proteção de Dados:
Stella Campos

Diretora do Núcleo de Prática da Comissão de Proteção de Dados:
Elaine Guerra

Membros do Núcleo de Prática:
Alan de Souza Pinto
Alessandra Campanha Puig Casariego
Carlos Henrique Almeida Salgado
Elaine Cristina Pereira dos Santos Nery
Emily Matias Assumpção
Gabriel Campos Cunha
Izabela Nunes Pinto
Priscila Silva Ribeiro
Renato Almeida Viana

Arte e Diagramação:
EQUIPE UAI-T
Crédito das imagens: https://www.freepik.com/

Versão 1.0
Publicação Digital (Dezembro de 2022)

INTERAJA COM A COMISSÃO DE PROTEÇÃO DE DADOS PESSOAIS DA OAB-MG
Instagram: @comissãolgpdoabmg
Facebook:
LinkedIn:
Youtube:
E-mail: protecaodedados@oabmg.org.br

SUMÁRIO

PREFÁCIO

A Lei Geral de Proteção de Dados (LGPD) adveio da necessidade em um movimento global de resguardar o direito à privacidade, bem como de legitimar o cidadão para exercer maior grau de controle sobre o fluxo e o tratamento de suas informações pessoais.

Essa norma se preocupa com a imagem de uma pessoa natural (cidadão) e seu objetivo maior é garantir a transparência sobre como um dado será tratado. Visa, também, dar autonomia ao cidadão para que este conceda ou não o uso do dado por uma pessoa de direito público ou privado.

Nesta cartilha exploraremos os principais tópicos e conceitos para entender a LGPD, como esta lei afeta a sua vida e o seu trabalho e principalmente auxiliar profissionais e instituições que desejam entender melhor o contexto da LGPD com o objetivo de aplicá-la na atuação da Privacidade e Proteção de Dados. Vamos conhecê-la?

ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

APRESENTAÇÃO DA OBRA

A presente cartilha foi elaborada pelo Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG, de forma clara e objetiva, para orientar os colegas advogados quanto à aplicação da Lei Geral de Proteção de Dados Pessoais – LGPD, haja vista que sempre surgem muitas dúvidas na adequação e implementação de uma nova lei.

1 - OBJETIVO DA CARTILHA

O presente material foi criado com o objetivo de levar aos profissionais que atuam ou desejam atuar na área de privacidade e proteção de dados, informações, conceitos, questões práticas e análises inerentes ao tema e, sobretudo, referentes à Lei Geral de Proteção de Dados Pessoais – LGPD, Lei 13.709/2019.

Este material pode ser utilizado por organizações que desejam entender melhor o contexto de aplicação da LGPD para aprimorar sua gestão sobre dados pessoais ou mesmo iniciá-la.

O objetivo deste material não é esgotar o tema, mas sim, tratar dos seus aspectos fundamentais, que precisam ser levados em conta para a aderência à LGPD e, principalmente, promoção da privacidade e segurança da informação.

2 - O QUE É A L.G.P.D?

A Lei Geral de Proteção de Dados ou LGPD foi sancionada em 14 de agosto de 2018, entrando em vigor após dois anos de vacatio legis em 14 de agosto de 2020, sendo efetivada suas sanções administrativas a partir de agosto de 2021.

Esta lei regula o tratamento dos dados pessoais nos âmbitos físicos e digitais, para fins comerciais, com o objetivo de resguardar os Direitos Fundamentais das pessoas físicas, direitos de privacidade, interesse, liberdade dos titulares dos dados e transparência no tratamento de dados, coibindo o tratamento de forma desmoderada e abusiva dos seus dados pessoais.

3 - PRINCIPAIS OBJETIVOS DA LGPD

Os principais objetivos trazidos pela Lei Geral de Proteção de Dados Pessoais são: proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos 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.

4 - FUNDAMENTOS DA LGPD

A LGPD se baseia em 7 fundamentos que disciplinam a Proteção dos Dados Pessoais, sendo eles:

FUNDAMENTOS	COMENTÁRIOS
O respeito à privacidade.	Assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada (art. 5º, X da CR 1988)
A autodeterminação informativa.	Assegurar o direito do titular de dados pessoais, o controle do tratamento destes dados e garantir sua proteção. Vale saber que a LGPD exclui em determinadas situações a prerrogativa da autodeterminação informativa.
A liberdade de expressão, de informação, de comunicação e de opinião.	Assegurar as liberdades de expressão dispostas no art. 5º, IV e IX da constituição federal: "IV - é livre a manifestação do pensamento, sendo vedado o anonimato;" "IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença"
A inviolabilidade da intimidade, da honra e da imagem.	Reforço o respeito à privacidade já disposto anteriormente.
O desenvolvimento econômico e tecnológico e a inovação.	Estimular o desenvolvimento setorial e tecnológico com ferramentas, soluções, serviços e novos processos que visam a promoção da privacidade e da segurança da informação.
A livre iniciativa, a livre concorrência e a defesa do consumidor.	Busca conferir segurança jurídica às atividades, deixando claro e disciplinando como o tratamento de dados pessoais pode ser realizado inclusive na interlocução com outras áreas do direito.
Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	Alinhar o tratamento de dados pessoais deve estar alinhado com os direitos e liberdades fundamentais como mecanismo de proteção do titular e promoção dos direitos à privacidade e de proteção dos dados pessoais

5 - ATORES ENVOLVIDOS E RESPONSABILIDADES

ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

A LGPD traz alguns atores fundamentais, sendo que cada um tem o seu papel, sendo esse o fundamento para o devido enquadramento e responsabilidades frente aos titulares dos dados.

Titular:
Diz respeito à pessoa física a quem se refere o tratamento dos dados pessoais. A título de exemplo, o titular do dado pode ser um cliente do escritório de advocacia, um cliente da padaria; um colaborador, um paciente, uma atendente, entre outros.

Responsabilidade do Titular dos Dados:
O titular dos dados também possui responsabilidades em relação ao tratamento dos dados pessoais, da mesma forma que os agentes de tratamento (Controlador e Operador). Todavia, cada um com sua responsabilidade.

- Seguir todas as normas de privacidade e proteção dos dados pessoais;
- Seguir e acompanhar os treinamentos;
- Cuidar com zelo dos dados pessoais dos titulares, dentre outras normas contidas nas Políticas da Organização.

Controlador:
É toda pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Responsabilidade do Controlador:
O Controlador detém diversas responsabilidades, e abaixo listamos apenas algumas a título de exemplo.

- Controlar como os dados serão coletados e usados;
- Definir quais dados serão coletados;
- Define por quanto tempo esses dados serão retidos;
- Definir com quem os dados serão compartilhados;
- Definir as medidas de seguranças que serão aplicadas;
- Realizar auditoria nos Operadores dos Dados;
- Determina quem tem o acesso a esses dados.

Operador:
É toda pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Responsabilidade do Operador:
O Operador também possui diversas responsabilidades e abaixo listamos alguns exemplos.

- Seguir as instruções do controlador;
- Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- Dar ciência ao controlador em caso de contrato com suboperador.

Não obstante as limitações acima, os operadores são livres para decidir quais sistemas, métodos e ferramentas aplicar para coletar dados e definir como eles são armazenados. Ex.: Parceiros comerciais contratados pelo escritório de advocacia, como a contabilidade.

Atenção: Aqueles que integram a empresa (do operador) em suas atribuições operacionais não são identificadas enquanto operador, a citar: empregados, administradores, sócios, servidores e outras pessoas naturais

Logo, o Operador em nada se confunde com o Controlador, tampouco sendo um profissional interno deste.

6 - A LGPD APLICA-SE A QUEM?

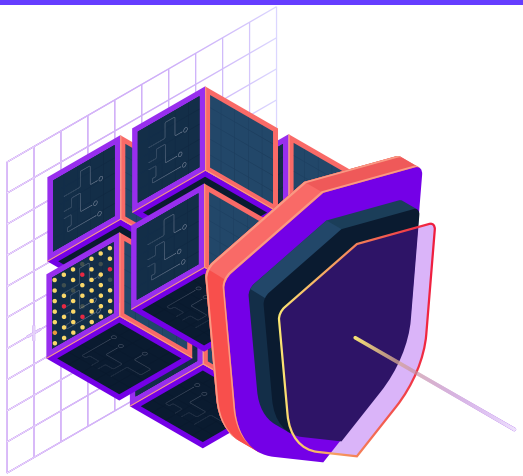
A LGPD aplica-se a todo tipo de empresa que realiza o tratamento de dados pessoais em território nacional, e às pessoas físicas que realizam o tratamento de dados com a finalidade econômica.

É importante entender que independente do porte da empresa, se esta realiza o tratamento de dados pessoais, deve se submeter à LGPD.

Para melhor exemplificar, o Microempreendedor individual – MEI que possui apenas 5 empregados e trata dados pessoais, deve se adequar à LGPD, do mesmo modo, um pequeno escritório de advocacia. Vale dizer que a Autoridade Nacional de Proteção de Dados - ANPD publicou a Resolução nº2/2022, constando as diretrizes do tratamento de dados para agentes de pequeno porte.

É imprescindível que você saiba quem deve se adequar à LGPD para elaborar um plano de adequação de acordo com a realidade de cada empreendedor.

7 - EXISTE ALGUMA EXCEÇÃO PARA NÃO APLICAÇÃO DA LGPD NO BRASIL?



Importante destacar que o tratamento de dados pessoais regulados pela LGPD tem foco nas atividades tem proveito econômico pelo controlador e operador e em atividades inerentes à promoção de políticas públicas, salvo àquelas ligadas à segurança pública.

Ou seja, dados pessoais que forem tratados:

- por pessoais naturais, sem que exista uma finalidade econômica;
- que forem tratados para fins jornalísticos ou artísticos;
- que forem tratados com finalidade acadêmica (sem fins diretamente comerciais), não serão aplicados os termos da LGPD, conforme disposto em seu art. 4º.

Conforme mencionado, a LGPD também não será aplicada no exercício, pelo Estado, das funções inerentes à:

- Segurança Pública;
- Defesa Nacional;
- Segurança do Estado; e
- Atividades de Investigação e Repressão de Infrações Penais.

Vale dizer, que o Artigo 4º, § 1º da LGDP prevê que uma legislação específica (ainda inexistente) deverá reger o tratamento de dados pessoais pelo Poder Público para as finalidades de segurança acima citadas dispondo de medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na própria LGPD.

A última hipótese trazida no artigo 4º, quanto a não aplicabilidade da LGPD, está disposta no inciso IV, e se refere a dados pessoais "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei".

Ademais, se uma empresa brasileira (operadora), prestando serviços para empresa estrangeira (controladora), "devolver" os dados pessoais eventualmente tratados ao país de origem, não será aplicável à LGPD, desde que tal país tenha uma legislação de proteção de dados adequada. Caso a empresa contratante esteja na União Europeia, por exemplo, neste caso, aplicar-se-ia o GDPR (Regulamento Europeu), e não a LGPD.

8 - O QUE SÃO DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS?

8.1 Dados Pessoais

Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável (art. 5º, I, da LGPD). A título de exemplo, dados pessoais são: nome, carteira de identidade, CPF, telefone, endereço residencial, prontuário de saúde, dados bancários e inscrição nos órgãos de classe.

Quando a lei menciona "informação relacionada à pessoa natural identificada", ela está referindo-se às informações relativas à pessoa (ser humano dotado de capacidade), que permitem diretamente a sua identificação.

Já a "informação relacionada à pessoa natural identificável" é toda aquela que tem o potencial de tornar a pessoa identificada. Exemplo: Advogado do Escritório XYZ, de 36 anos, que faz aniversário em abril. Se houver apenas um advogado que preencha essas características, essas informações serão suficientes para identificá-lo. Outro exemplo é a placa de um carro – Só de olhar a placa, via de regra, você não consegue identificar o titular – você precisa de informações adicionais para saber quem realmente é o proprietário do veículo.

Segundo o art. 12, § 2º, da LGPD, poderão ser igualmente considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Quando a lei cita "formação do perfil comportamental", ela está fazendo referência ao "tratamento dos dados pessoais coletados, que permitem que terceiros analisem os interesses, preferências e até mesmo o preço que o indivíduo quer pagar por determinado produto ou serviço."

8.2 Dados Pessoais Sensíveis

Dispõe o art. 5º, II, da LGPD, que dado pessoal sensível refere-se ao 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 a uma pessoa natural.

Considerando a natureza dos dados pessoais sensíveis, o art. 11 da LGPD estabelece que o seu tratamento somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
cumprimento de obrigação legal ou regulatória pelo controlador;
execução, pela administração pública, de políticas públicas;
realização de estudos por órgão de pesquisa;

d) exercício regular de direitos;
e) proteção da vida ou da incolumidade física;
f) tutela da saúde;
g) garantia da prevenção à fraude e à segurança do titular.

Além das hipóteses listadas nos incisos I e II do artigo 11 da Lei, o referido artigo também determina às entidades públicas que tratarem de dados sensíveis para cumprimento de obrigação legal ou regulatória, bem como para a execução de política pública deverão dar ampla publicidade à dispensa de consentimento nos termos do art. 23 da LGPD (art. 11, §2º).

Ademais, o §3º do art. 11 da LGPD dispõe que a comunicação ou uso compartilhado de dados pessoais sensíveis entre controladores com o objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional.

O §4º veda a comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o §5º do mesmo artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares e para permitir:
a portabilidade de dados quando solicitado pelo titular, ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Conforme exposto, a LGPD não trata de qualquer tipo de dado, mas tão somente de dados pessoais, sendo que os dados pessoais sensíveis, por potencialmente envolver risco de discriminação ou vulnerabilidade aos direitos do seu titular, recebem tratamento especial estabelecido no artigo 11 da LGPD.

9 - O QUE É BANCO DE DADOS?

Banco de dados é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, conforme estabelece o art. 5º, IV da LGPD. Portanto, o dado pessoal será protegido independentemente do meio (físico ou digital).
É importante esclarecer a diferença entre base de dados, banco de dados e dados.

Nesse sentido, o ilustre Rony Vainzof (2018) arrazoa que:

(...) enquanto as bases de dados são devidamente protegidas por direitos autorais, desde que observados critérios de seleção e organização, em que a compilação dos dados constituírem criação intelectual, dados em si não guardam proteção autoral, mas são tutelados por diferentes formas, pois, de acordo com a sua sensibilidade e tratamento, podem ferir outros importantes direitos, como o da intimidade, da vida privada, da honra e da imagem das pessoas. Quando tais dados que identificam ou possam identificar uma pessoa estão estruturados conjuntamente, formam o conceito de banco de dados pessoais.

Por fim, e como dica de ouro, em se tratando de dados pessoais, menos é mais! Deve-se avaliar a real necessidade do tratamento do dado pessoal. Quanto menos dados forem coletados, melhor. A coleta indiscriminada de dados pessoais pode representar custos financeiros e riscos desnecessários. A definição de uma política de retenção determinando por quanto tempo cada dado pessoal deve ser mantido é fundamental.

ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

10 - O QUE É ENCARREGADO DE PROTEÇÃO DE DADOS E QUAIS SUAS FUNÇÕES?

O Data Protection Officer (DPO), trazido para a LGPD como Encarregado de Proteção de Dados é a pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Em 29 de julho de 2021, a ocupação de DPO/Encarregado pelo Tratamento de Dados foi incluída e reconhecida oficialmente no CBO – Classificação Brasileira de Ocupações. Logo o cargo já é uma realidade nas empresas brasileiras.

A LGPD traz no seu artigo 41 as principais atividades do Encarregado de dados, sendo elas:

§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

A ANPD ainda não publicou nenhuma regulamentação sobre as demais atribuições do Encarregado de Proteção de Dados (DPO). Todavia, na prática, os Encarregados estão desempenhando o papel de:
Orientação para o desenvolvimento do projeto de adequação;
Treinamento dos colaboradores para conscientização da cultura de proteção de dados;
Orientação para adequação das políticas;
Orientação para adequação da infraestrutura interna (TI);
Orientação para adequação dos contratos com fornecedores, prestadores de serviço e clientes;

Nota-se que o Encarregado de Proteção de Dados representa a empresa no que diz respeito à proteção de dados, bem como desempenha um papel de gestão nos processos acima citados.

Por fim, ainda existem muitas especulações sobre o papel do Encarregado, se deve ser executado por um profissional de Segurança da Informação ou pelo Corpo Jurídico, se tem que ter certificações ou não, mas, uma coisa é certa, o papel do Encarregado de dados exige muito e ainda dá muito trabalho, visto que no Brasil as empresas ainda não detêm uma cultura enraizada de privacidade e proteção dos dados pessoais.

11 - QUAIS SÃO OS PRINCÍPIOS TRAZIDOS PELA LGPD?

O artigo 6º da LGPD traz os princípios que servem como um alicerce para a garantia e efetivação da LGPD.

Finalidade
Para todo tratamento de dados pessoais é preciso ter uma finalidade específica.

Adequação
O tratamento dos dados pessoais deve ser realizado em compatibilidade, com a finalidade, necessidade e adequação à legislação.

Necessidade
Somente os dados que são necessários para a finalidade específica devem ser tratados, com o objetivo de minimizar os danos.

Livre acesso
É necessário garantir a efetivação dos direitos dos titulares sobre seus dados, dando-lhes livre acesso, a chamada autodeterminação informativa.

Qualidade dos dados
Garantia ao titular de exatidão, clareza, relevância transparência e atualização dos dados.

Transparência
Esse princípio é uma das bases norteadoras da proteção de dados, assegurando informações objetivas, precisas e de fácil acesso a seus dados.

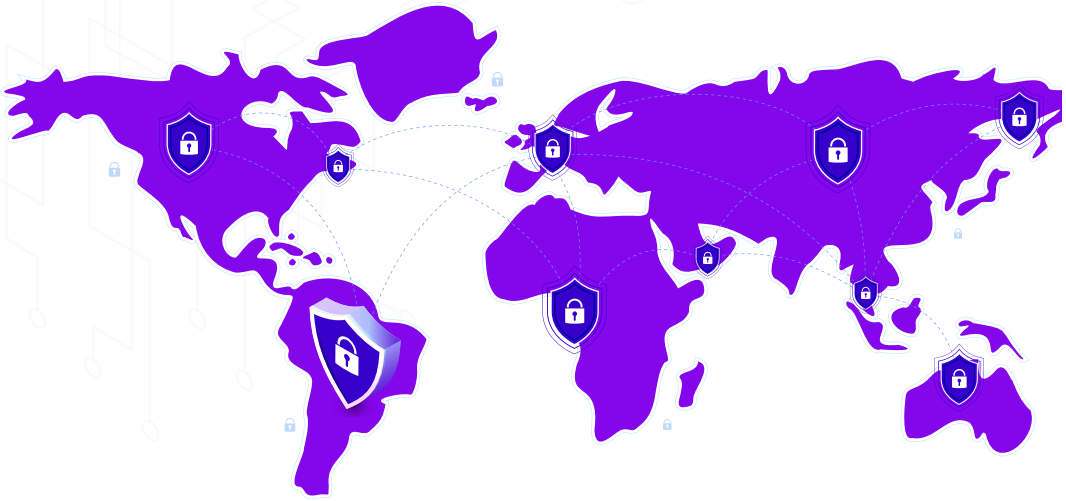
Segurança
É importante que a empresa tenha meios seguros para garantir a proteção dos dados pessoais, a fim de minimizar incidentes de segurança.

Prevenção
A empresa deve adotar medidas para prevenir a ocorrência de danos aos titulares dos dados pessoais, como programa de governança de privacidade e prevenção de mitigação de riscos.

Não Discriminação
É vedado que o tratamento dos dados pessoais tenha finalidade discriminatória, abusiva ou ilícita.

Responsabilização e Prestação de Contas
É importante que a empresa possua meios de comprovação com as evidências de conformidade, documentos, dentre outros.
Após entender quais são os princípios e seus objetivos, vale dizer que não existe um processo de adequação à LGPD bem-sucedido que não siga os princípios listados acima, todas suas fases devem estar em conformidade com a Lei.

12 - O QUE É CONSIDERADO TRANSFERÊNCIA INTERNACIONAL DE DADOS?



ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

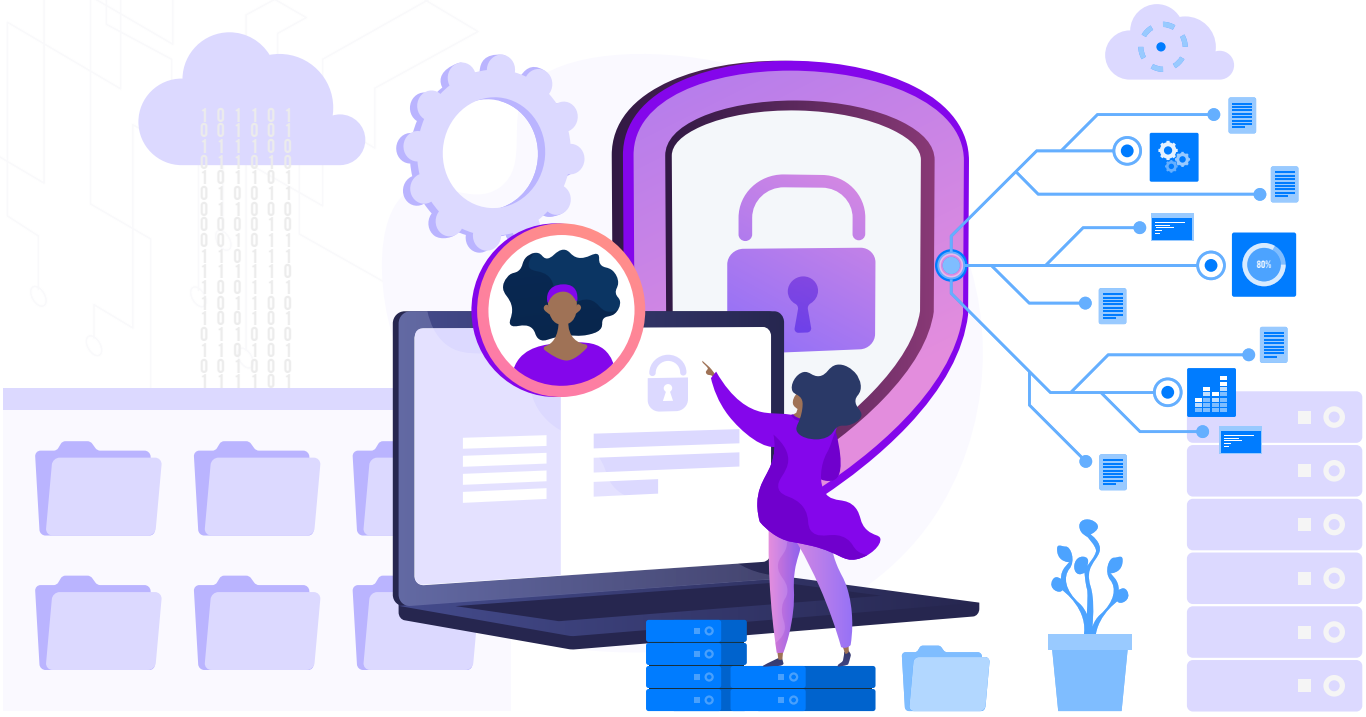
Nos termos do artigo 5º, XV da LGPD, é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Isso acontece devido à atividade de determinado Controlador precisar tratar dados pessoais em suas unidades em outros países ou com outros controladores (ex.: parceiros comerciais, órgãos públicos ou outras instituições) ou, ainda, que contratam serviços realizados por operadores, fora do Brasil (ex: armazenamento de dados em nuvem).
Havendo transferência internacional de dados, o responsável pelo tratamento deve respeitar os princípios de proteção de dados e garantir os direitos dos titulares. A LGPD traz em seu artigo 33 as hipóteses e condições em que a transmissão de dados é permitida.

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

É fundamental que as organizações verifiquem todas as situações em que suas atividades e processos, mesmo que secundários, possam realizar a transferência de dados pessoais para outros países (Armazenamento em nuvem). É bom enfatizar, que todas as circunstâncias mapeadas devem estar devidamente amparadas por hipótese ou condição disposta no art. 33 citado. Caso não estejam, é necessária a elaboração de plano de ação para adequação.

13 - QUEM É O TITULAR DOS DADOS?

A LGPD identifica o titular de dados como sendo todo pessoal natural a que se refere os dados pessoais que são objeto de tratamento, ou seja, o titular dos dados é VOCÊ, sou EU, somos NÓS.



14 - O TITULAR DOS DADOS TEM ALGUM DIREITO?

A LGPD traz direitos aos titulares de dados a fim de assegurar a privacidade, intimidade e demais direitos fundamentais. Desse modo, o titular dos dados tem a legitimidade de requerer do agente de tratamento dos dados, a qualquer momento, o direito de:

DIREITO / EXPLICAÇÃO

Revogar o consentimento
Diz respeito à hipótese de o tratamento dos dados justificar tão somente a livre manifestação de vontade do titular dos dados, podendo este fazer a sua interrupção, a qualquer momento.

Informação
Direito do titular de dados de confirmar a existência de tratamento de seus dados pessoais, devendo informar o agente de tratamento; encarregado/ DPO; existência ou não de compartilhamento; informar os direitos.

Acesso aos dados
Ter conhecimento de como o tratamento está sendo realizado a comunicar: finalidades, categorias, destinatários, prazo de conservação, origem dos dados, existência de decisões automatizadas.

Retificação dos dados
Possibilidade de correção dos dados, observando a necessidade e para o cumprimento da finalidade de seu tratamento.

Eliminação
Alternativa para o titular dos dados remover os seus dados pessoais, nos casos de: não são mais necessários para a finalidade; titular revoga o consentimento; ilegalidade de tratamento; cumprimento de obrigações legais.

Oposição
Direito de se opor ao tratamento quando a base legal de tratamento não tiver seu consentimento ou em desacordo com o que é estabelecido pela LGPD.

Portabilidade de dados
Direito de solicitar que seus dados pessoais sejam fornecidos a ele, em um formato estruturado e legível, e transferir esses dados para outro agente de tratamento.

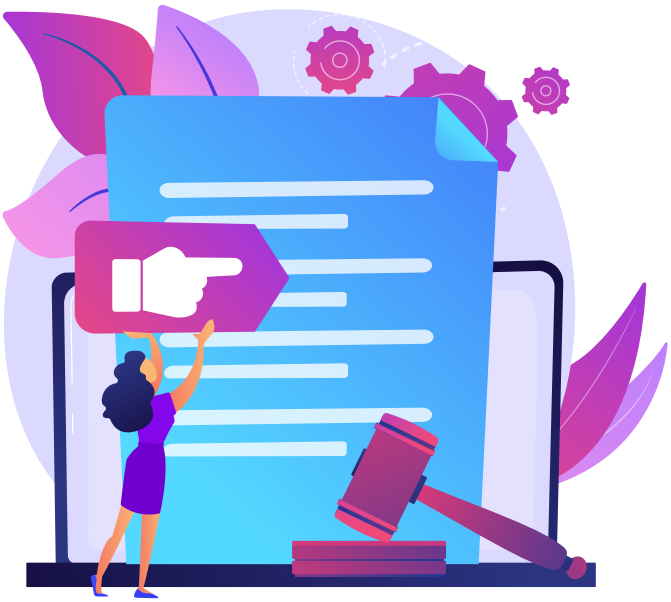
Automação de decisões
Direito de não se sujeitar a decisões com perfis automáticos, quando a decisão tenha um efeito significativo, podendo insistir na intervenção humana, quando adequado.

Reclamar à ANPD
Direito de o titular dos dados peticionar apresentando questionamento a respeito de qualquer ponderação em relação ao tratamento de seus dados pessoais perante à ANPD.

Anonimização
Não poder mais identificar o seu titular, ou seja, dissociar os dados pessoais à sua identificação, quer seja direta ou indireta.

Bloqueio
Restrição ao direito de tratamento dos dados desnecessários e excessivos ou tratados em desconformidade com a LGPD.

15 - COMO O TITULAR DOS DADOS PODE SOLICITAR SEUS DIREITOS?



ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

Conforme mencionado no item anterior, os titulares dos dados detêm diversos Direitos descritos na LGPD. Para melhor compreensão, elaboramos a título de exemplo, os quadros abaixo esclarecem algumas dúvidas e resposta sobre as solicitações dos direitos dos titulares dos dados perante o Controlador e a ANPD.

Como podem ser feitas as requisições de informações pelo Titular de dados ao Controlador?
O Titular de dados poderá entrar em contato com o Controlador de dados por meios dos canais oficiais, como e-mails, pelo site do Controlador, pelo aplicativo, nas redes sociais, diretamente no endereço físico do Controlador, sendo recomendável que o titular de dados guarde os dados do contato, como, por exemplo, número de protocolo, orientações recebidas, mensagens e e-mails entre outros.

O titular de dados pode requerer diretamente à ANPD a resolução de suas demandas?
Via de regra, não. O titular dos dados antes de demandar junto à ANPD, deverá solicitar formalmente ao Controlador seus requerimentos.

A LGPD estabelece no Art.18 § 1º e 3º que o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional.
Todavia, para que o titular dos dados apresente à ANPD sua reclamação, primeiro, deverá comprovar que já contactou o Controlador - e esse, não atendeu a sua solicitação. Além do mais, deverá demonstrar que não ficou satisfeito com a solução apresentada pelo Controlador. A recomendação é que o titular dos dados junte prova nos autos para demonstrar que o Controlador não atendeu a sua solicitação (Ex.: Número do Protocolo/solicitação).

Como peticionar junto à ANPD?
O titular dos dados poderá peticionar junto à ANPD através dos canais de atendimento ao cidadão/titular de dados: https://www.gov.br/anpd/pt-br.

Após o recebimento pela ANPD como ocorre a análise da petição do Titular de dados?
Na LGPD Art. 55, V, §6 aduz que a ANPD tem competência para apreciar as petições do Titular contra o Controlador após comprovada pelo Titular a apresentação de reclamação ao Controlador não solucionada no prazo estabelecido em regulamentação, sendo que as reclamações colhidas poderão ser analisadas, de forma agregada e as eventuais providências dela decorrentes, poderão ser adotadas de forma padronizada.

16 - QUAIS AS SANÇÕES QUE AS EMPRESAS PODEM SOFRER SE NÃO ATENDEREM AOS DIREITOS DOS TITULARES DOS DADOS?

Desde agosto de 2021, as empresas que não efetivarem os direitos dos titulares podem sofrer as penalidades previstas no art.52 da LGPD, sendo elas:

Advertência, com indicação de prazo para adoção de medidas corretivas;
Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
Multa diária, observado o limite total a que se refere o inciso II;
publicização da infração após devidamente apurada e confirmada a sua ocorrência;
Bloqueio dos dados pessoais a que se refere a infração 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 pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

É importante destacar que as penalidades acima elencadas através de procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com o caso concreto, conforme previsto na LGPD e mais Normativas da ANPD.

Vale dizer que a "famosa" multa de a R$50.000.000,00 (cinquenta milhões de reais) por infração, por vezes pode não ser pior se comparada à publicização do ato, que compromete a reputação da empresa diante da disseminação do "Tribunal da Internet".

O que devemos sempre alertar enquanto consultores em proteção de dados é que um processo de adequação e implementação da LGPD iniciado de forma preventiva acautela a aplicação das penalidades em questão.

ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

17 - O QUE MINHA EMPRESA PRECISA FAZER EM CASO DE UM INCIDENTE DE SEGURANÇA?

Inicialmente, espera-se que as empresas estejam preparadas para solucionar quaisquer crises que surjam em caso de incidentes de Segurança. Todavia, caso a empresa adote todas as medidas de segurança, e mesmo assim, venha ocorrer um incidente, essa, deverá de imediato colocar em prática o plano de resposta e, em paralelo, abrir um processo interno para verificar como e por que ocorreu o vazamento de dados pessoais dos usuários.

O capítulo VII da LGPD, fala sobre a segurança e boas práticas, apontando as medidas que deverão ser adotadas para proteger os dados pessoais de acessos não autorizados, sendo que o Controlador deverá comunicar à ANPD e ao Titular a ocorrência de incidente

Art. 46. Os agentes de tratamento 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.

O artigo acima mencionado aduz que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a resguardar os dados pessoais de atos que possam provocar algum tipo de incidente de segurança, todavia, a LGPD não menciona quais são essas medidas técnicas e administrativas. Entretanto, as empresas vêm adotando como medidas técnicas e administrativas a aplicação das Normas ISO 27001, 27701, 27002, 3100 entre outras para tentar mitigar os incidentes.

18 - O QUE É TRATAMENTO DE DADOS?

O art. 5º inciso X, da LGPD estabelece que o tratamento é toda operação realizada com os dados pessoais, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
A LGPD trouxe diversas expressões que caracterizam o tratamento dos dados pessoais, mas, resumidamente, o tratamento seria o ciclo de vida, ou o processo que descreve o caminho dos dados dentro da sua organização, desde o momento em que é coletado até a sua eliminação/descarte.
Como exemplo, sua empresa coleta os dados para admissão de um colaborador, armazena esses dados através de softwares ou pastas, compartilha esses dados com a contabilidade para geração de folha de pagamento, e por fim, elimina após o desligamento do colaborador.

19 - TENHO OUVIDO MUITO SOBRE O CICLO DE VIDA DOS DADOS! O QUE SERIA?

A Lei Geral de Proteção de Dados (LGPD) traz novos desafios para o processamento de dados estando dentre eles, a implementação da gestão do ciclo de vida dos dados. O ciclo de vida dos dados nada mais é do que o processo que descreve o caminho dos dados dentro da organização (empresa, escritório), desde o momento em que o dado é coletado (em conformidade com a(s) base(s) legal(is) indicadas no Art. 7º) até o arquivamento ou eliminação deste.

O ciclo de vida dos dados apresenta as seguintes etapas:

Sendo que:

Coleta
significa a obtenção, recepção ou criação dos dados pessoais, seja por meio físico ou eletrônico/digital.

Retenção/Armazenamento
significa o armazenamento ou arquivamentos dos dados pessoais, independentemente do meio utilizado (físico ou eletrônico).

Processamento
significa qualquer operação que envolva utilização, classificação, reprodução, processamento, análise, avaliação, extração, modificação de dados pessoais.

Compartilhamento
significa qualquer operação que envolva transmissão, distribuição, transferência, comunicação, difusão ou compartilhamento de dados pessoais.

Reutilização
significa realizar o processamento ou compartilhamento dos dados pessoais, novamente.

Eliminação
significa qualquer operação que tenha por finalidade apagar ou eliminar os dados pessoais.

Em suma, a gestão ou gerenciamento do ciclo de vida dos dados é o conjunto de princípios de governança que visam definir e automatizar os estágios da vida útil dos dados, desde a criação à eliminação, determinando a sua priorização.

Em termos mais simples, antes de realizar quaisquer coletas de dados, a empresa deve elaborar as seguintes perguntas:

As informações coletadas são relevantes, precisas e possuem uma finalidade específica e legítima de uso?
Quando essas informações deverão ser eliminadas?

Nesse contexto, a gestão do ciclo de vida dos dados deve ser incorporada ao negócio, considerando a finalidade do fornecimento de seus bens e serviços.

A seguir, disponibilizamos um quadro explicativo de cada fase do ciclo de vida dos dados, em conformidade com a LGPD:

FASES DO CICLO	COMO ERA ANTES DA LGPD?	COMO É COM A LGPD?
COLETA	Dados coletados de forma indiscriminada.	A coleta de dados pessoais deve obedecer aos princípios da LGPD, dentre eles aos princípios da necessidade e finalidade.
RETENÇÃO ARMAZENAMENTO	Os dados pessoais são armazenados e mantidos por prazo indefinido.	Todo dado pessoal armazenado, seja em digital ou fisicamente, carece de prazo de vida.
PROCESSAMENTO	Não há necessidade de um tratamento específico para o processamento dos dados pessoais.	O processamento dos dados pessoais somente pode ser realizado nas hipóteses do Art. 7º da LGPD.
COMPARTILHAMENTO	O compartilhamento dos dados pessoais não exige o consentimento ou outra base legal que o justifique.	O compartilhamento dos dados pessoais pressupõe propósitos legítimos e específicos e deve cumprir todos os requisitos e procedimentos da LGPD.
REUTILIZAÇÃO	A reutilização dos dados pessoais não exige o consentimento ou outra base legal que a justifique.	A reutilização dos dados pessoais pressupõe propósitos legítimos e específicos e deve cumprir todos os requisitos e procedimentos da LGPD.
ELIMINAÇÃO	Os dados pessoais podem ser mantidos sem a obrigatoriedade da eliminação.	Após o término do tratamento, os dados pessoais devem ser eliminados.

20 - QUAIS SÃO AS BASES LEGAIS PARA O TRATAMENTO DOS DADOS?

A LGPD prevê em seus artigos 7º e 11º as possibilidades para o tratamento de dados pessoais. Esses dois artigos detém as chamadas bases legais.

No artigo 7º são previstas 10 possibilidades de tratamento de dados pessoais que não sejam os dados pessoais sensíveis, pois esses estão descritos no artigo 11º.

As 10 bases legais que permitem o tratamento dos dados pessoais, são:

Consentimento do titular do dado

Esta base legal considera a autonomia da vontade do titular de dados pessoais que, de forma livre, concorda com o tratamento dos seus dados pessoais para uma finalidade determinada e previamente informada. Destaca-se que o titular que autorizou o tratamento de seus dados pessoais pode revogar esse consentimento a qualquer momento.

Nos termos do art. 7º da LGPD é dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na lei.

Quando o tratamento de dados pessoais tem como fundamento o consentimento do titular o controlador só pode compartilhar esses dados com outros controladores com consentimento específico para tal, ressalvadas as hipóteses de dispensa do consentimento previstas em Lei.

Para o cumprimento de obrigação legal ou regulatória pelo controlador

Essa base legal, assim como as seguintes, dispensa o consentimento do titular do dado. Trata-se da prevalência do interesse público sobre o particular, uma vez que, independentemente da vontade do titular, seus dados podem ser tratados pelo controlador para o cumprimento do disposto em leis e normas.

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

Trata-se de hipótese de tratamento de dados pessoais com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo. Mesmo sendo dispensado o consentimento do titular para o tratamento de dados, é obrigatório que seja informada a finalidade e a forma como o dado será tratado.

Para a realização de estudos por órgão de pesquisa, é garantida, sempre que possível, a anonimização dos dados pessoais

Esta hipótese de tratamento também dispensa o consentimento do titular. Entretanto, a utilização dos dados é restrita para realização de estudos por órgão de pesquisa público ou privado.

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

Hipótese que dispensa novo consentimento do titular, desde que: (a) o tratamento de dados em questão seja imprescindível para o devido cumprimento do contrato; e (b) o titular dos dados tenha previamente manifestado consentimento, na celebração do contrato.

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Esta hipótese de tratamento compatibiliza as diretrizes da LGPD com o direito constitucional de acesso à justiça (art. 5º XXXV). Ou seja, a proteção aos dados pessoais não compromete o direito de se demandar ou defender judicialmente, administrativamente e em instancias arbitrais, mesmo que a produção de provas, por exemplo, seja composta por dados pessoais da parte contrária.

Para a proteção da vida ou da incolumidade física do titular ou de terceiros.

O tratamento de dados pessoais nesta hipótese dispensa o consentimento do titular uma vez que a tutela do bem da vida se sobrepõe.

Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Hipótese que dispensa o consentimento do titular do dado nos casos de estrita necessidade de tutela da saúde do titular, de terceiro ou pública. É a única hipótese de tratamento de dado manejado por agente exclusivo: profissionais de saúde, serviços de saúde ou autoridade sanitária.

Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Com fundamento nessa base legal, o tratamento de dados pessoais dispensa o consentimento do titular. Entretanto, essa base legal só pode ser utilizada em determinadas situações e o controlador assume toda a responsabilidade sobre o uso dos dados. Nos termos do art. 10º da GPD o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador;

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD. Em tais circunstâncias, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo o controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. Convém salientar que o tratamento autorizado por esta hipótese traz consigo conjunto adicional de medidas de salvaguarda dos dados, inclusive com a possibilidade de a ANPD solicitar ao controlador relatórios de impacto à proteção de dados pessoais, justamente pelo risco de violação que tal hipótese acarreta, em particular, para entidades privadas. A elaboração do referido relatório de impacto é abordada na seção 2.5 deste documento.

Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Nesta hipótese, em que também se dispensa o consentimento, o tratamento de dados pessoais pode ser realizado para realizar cobranças, conceder crédito e outras atividades financeiras correlatas ao tema realizadas pelo controlador.

Já o artigo 11º da LGPD conforme mencionado, traz a listagem de bases legais para o tratamento de dados sensíveis, sendo elas:

Base Legal
Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas

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

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

21 - PSEUDONIMIZAÇÃO, ANONIMIZAÇÃO E DADO ANONIMIZADO

De acordo com o art. 5º, III, da LGPD, o dado Anonimizado é o "...relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Já a Anonimização é conceituada como sendo a utilização desses meios, pelos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, conforme disposto no art. 5º, XI da LGPD.

Na prática, a empresa utiliza de meios técnicos (anonimização) e, após o procedimento, os dados ficam (anonimizados) e não podem ser identificados.

Uma vez anonimizados, os dados não são mais considerados pessoais, salvo quando o processo de anonimização for (ou puder ser) revertido, segundo o art. 12 da LGPD.

Base - Original

nome	e-mail	gênero	idade
Elaine Guerra	elaineguerra.adv@gmail.com	feminino	36 anos

Processo anonimizado - Passa por um processo de mascaramento

nome	e-mail	gênero	idade
xxxxxxxxxx	xxxxx@xxxx.com	feminino	36 anos

Já a pseudonimização é uma técnica diferente da anonimização explicada anteriormente. Essa, segundo o art. 13, §4º, da LGPD, é o dado que "perdeu, pelo tratamento, a possibilidade de associação, direta ou indireta, a um indivíduo, pelo uso de informação adicional mantida separadamente em ambiente controlado e seguro".

Cada organização deverá avaliar qual técnica atenderá sua demanda.

Base - Original

nome	e-mail	gênero	idade
Elaine Guerra	elaineguerra.adv@gmail.com	feminino	36 anos

No processo pseudonimizado, não irei mascarar os dados, mas separá-los em um sistema/tabela

nome	e-mail	referência
Elaine Guerra	elaineguerra.adv@gmail.com	123456

Exemplo: Nesta tabela, eu tenho o nome, e-mail e referência.

referência	gênero	idade
123456	Feminino	36 anos

Exemplo: Já neste outro sistema, eu tenho os dados separados em um ambiente seguro pelo controlador das informações. Esses dados são mantidos em base de dados separadas.

22 - POSSO TRATAR DADOS DE CRIANÇA E DE ADOLESCENTE?

A LGPD, em seu art. 14., dispõe que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse.

Entretanto, é importante entender a diferença entre criança e adolescente de acordo com o Estatuto da Criança e do Adolescente - ECA:

CRIANÇA	ADOLESCENTE
até doze anos incompletos	entre doze e dezoito anos

Vale dizer, que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico dado por pelo menos um dos pais ou pelo responsável legal.

Além disso, os controladores de dados deverão manter pública a informação sobre os tipos de dados coletados, em seus canais de comunicação (website ou WhatsApp), por e-mail, em sua Política de Privacidade, dentre outros.

A LGPD traz hipótese em que se aceita a coleta de dados pessoais de crianças sem o devido consentimento dos pais ou do representante legal, sendo:

- Quando a coleta do dado for necessária para contatar os pais ou responsáveis
- Quando para sua proteção

Vale mencionar, quando os dados forem utilizados sem o consentimento, como é o caso das exceções acima, devem ser utilizados uma única vez e sem armazenamento e em nenhum caso poderão ser repassados a terceiro sem o devido consentimento.

Ademais, o controlador deve adotar medidas técnicas e administrativas para verificar se o consentimento foi dado pelos pais ou responsáveis legais da criança, consideradas as tecnologias disponíveis pela Organização.

ANPD Autoridade Nacional de Proteção de Dados

23 - QUEM É A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E QUAL SUA FUNÇÃO/ COMPETÊNCIA?

A Autoridade Nacional de Proteção de Dados é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional.

Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;
II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;
XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
XII - elaborar relatórios de gestão anuais acerca de suas atividades;
XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;
XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;
XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;
XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;
XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Somado a isso, a LGPD institucionalizou a ANPD com o papel fundamental na interpretação e proteção dos dados pessoais. Assim, terá como objetivo orientar, mediante seu corpo técnico, sobre os limites do texto legal, cooperar com autoridades de controle, além de proceder com a realização de fiscalizações necessárias para o cumprimento da LGPD,

É bom enfatizar que a cultura de proteção de dados no Brasil ainda é um tema novo e caberá à ANPD promover a popularização e conhecimento sobre a matéria. Não será um trabalho fácil, mas a ANPD terá um papel fundamental para a transformação da cultura em toda a população.

24 - O QUE SERIA O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS?

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é definido pela LGPD (art. 5º, XVII) como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

> **Art. 5º: Para os fins desta Lei, considera-se**:
> (...)
> XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Vale destacar que, "a segurança dos dados pessoais tratados é uma obrigação legal geral imposta aos agentes de tratamento, e o RIPD insere-se neste contexto (1)". O supracitado artigo, traz a definição do que seria o RIPD, já o art. 38, parágrafo único da LGPD, esclarece abaixo o conteúdo mínimo do documento:

> **Art. 38.** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Além disso, a ANPD poderá solicitar o mesmo relatório quando o fundamento para tratamento do dado pessoal for o interesse legítimo, nos moldes do art. 10, §3º da LGPD.

> **Art. 10.** O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> (...)
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

A LGPD não especifica todos os parâmetros do relatório, porém, ao ser elaborado, o controlador deverá se atentar aos conceitos fundamentais trazidos pela lei, como a necessidade de descrever no relatório o fluxo de informação, o contexto do tratamento, a identificação dos riscos e as ações tomadas para mitigação desses riscos.

Outro ponto interessante é que o RIPD não é obrigatório para todas as empresas, uma vez que sua confecção não está determinada na lei, contudo, tendo em vista que se trata de uma ferramenta de gestão de riscos, bem como que a ANPD poderá solicitá-lo a qualquer momento, é importante que as empresas, quando da sua adequação, o elaborem, especialmente aquelas que tratam dados pessoais sensíveis e dados de crianças e adolescentes.

O relatório deve ser criado após profunda análise dos processos da organização, sendo aplicado quando o processamento traz altos riscos aos direitos e liberdades dos titulares de dados pessoais, e deve ser conduzido de forma eficiente por uma equipe multidisciplinar, envolvendo práticas de gestão de projetos, conhecimentos jurídicos e tecnológicos.

O relatório de impacto deverá conter, no mínimo:

- a descrição dos tipos de dados coletados;
- a metodologia utilizada para a coleta;
- a metodologia para a garantia da segurança das informações;
- a análise do controlador com relação a medidas, salvaguardas;
- mecanismos de mitigação de risco adotados.

O controlador deverá indicar um "encarregado" (DPO) pelo tratamento de dados pessoais, que são os responsáveis na prática por gerenciar o controle de dados, conforme as atribuições do art. 41, da LGPD.

O DPO será o responsável pela elaboração de um modelo para o relatório de impacto, conforme disposto na Lei. Vale destacar que, o responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

Elaborado o RIPD, este deverá ser submetido à aprovação por meio da obtenção das assinaturas do responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador.

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

25 - TENHO VISTO QUE DIVERSOS SITES ESTÃO MOSTRANDO UM AVISO SOBRE O USO DE COOKIES! PARA QUE SERVE? É NECESSÁRIO?

Como já visto nos tópicos anteriores, a mudança de Cultura de Proteção de Dados está em todos os meios e os sites com os avisos de Cookies é um deles. Atualmente, quando acessamos os sites para realizar uma pesquisa ou uma compra, já somos informados através de uma barra que o site coleta Cookies. Neste momento, temos a opção de aceitar, rejeitar, configurar e em alguns sites, até a opção de ler a Política que trata do tipo de Cookies que são coletados e tratados por aquela empresa.

Para melhor compreensão, o Guia explicativo lançado em outubro de 2022 pela ANPD trouxe o conceito do que seria Cookies, ou seja, "Cookies são arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas".

A LGPD não fala especificamente na palavra cookies, mas o artigo 5º é muito claro ao enfatizar o que seria um dado pessoal - I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável, ou seja, se as empresas através de suas plataformas conseguir coletar dados pessoais sem o consentimento do visitante, estarão sujeitas às penalidades prevista na LGPD. Por isso, as empresas estão configurando seus sites para dar mais transparência aos titulares dos dados, e passando para esses, o poder de decisão sobre seus dados pessoais.

A título de exemplificação, segue alguns tipos de cookies coletados através da sua navegação:

COOKIES DE ACORDO COM A ENTIDADE RESPONSÁVEL POR SUA GESTÃO

Cookie Persistentes ou Primários

Estes são armazenados em seu equipamento de navegação e utilizados para manter informações de escolhas realizadas no site, como, por exemplo, o idioma que você escolheu.

Dessa forma, quando você retornar ao site, estará no idioma selecionado anteriormente. Esses cookies não são excluídos ao fechar o navegador ou reiniciar seu aparelho. Geralmente possui um prazo de validade de um a dois anos, mas também é possível excluí-lo manualmente.

Cookie de Terceiros

Esse tipo de cookie não traz benefícios para o visitante do site. Esse tipo de ação captura seu perfil de consumo, informações de sua localização, informações sobre suas preferências e de seu equipamento. Essas são as maiores razões para tornar esses cookies como de má reputação.

Destarte, é necessário dar destaque aos cookies, o que são, o que fazem, possibilitando ao usuário fazer gerenciamento de permissões. "Segundo um relatório da União Europeia sobre proteção de dados que analisou 500 sites, 70% dos cookies são de terceiros e rastreiam nossa atividade para nos oferecer publicidade personalizada". É preciso informar aos usuários do site quais os tipos de cookies que o site utiliza e para que servem, possibilitando que o titular, caso queira, possa ajustar seus interesses aos cookies a partir de um clique, lembrando que não é possível desativar os cookies estritamente necessários.

COOKIES DE ACORDO COM A NECESSIDADE

Cookies necessários:

São utilizados pelos sites para que as funcionalidades básicas do site funcionem corretamente, tornando-o essencial, uma vez que a captura de informações assegura o bom desempenho da página. Esses Cookies quando desabilitados a página deixa de funcionar, impedindo a prestação do serviço oferecido.

Cookies não necessários:

São utilizados com objetivo de levar anúncios mais precisos aos usuários, no entanto precisa conseguir identificar comportamentos do seu público, as especificidades dos usuários permitem chegar à publicidade quase que personalíssima.

Desse modo, torna-se importante identificar a diferença entre esses cookies, para definir qual hipótese legal será utilizada para a coleta dos dados.

COOKIES DE ACORDO COM A FINALIDADE

Cookies analíticos ou de desempenho:

São utilizados com intuito de obter dados e informações sobre os usuários, como se comportam no site, seus gostos, a utilização do site e quais páginas mais visitam no dia a dia e até mesmo o próprio desempenho do site e ocorrência de erros nas páginas.

Cookies de funcionalidade:

São usados com objetivo de otimizar a visita do usuário, fornecendo serviços automatizados que facilitam suas buscas. Os maiores exemplos são do idioma do usuário que já é automático, seu nome em algumas páginas, a região e até mesmo preferências. Esse cookie pode ser classificado como persistente, próprios, de sessão e de terceiros.

Cookies de publicidade:

São desenvolvidos para coletar informações do usuário e a partir de seus hábitos lhes fornecerem produtos por meio de anúncios. Esse tipo de cookie constrói o perfil do usuário permitindo personalizar a entrega das informações que serão veiculadas por sua página.
Cookies de acordo com o período de retenção das informações

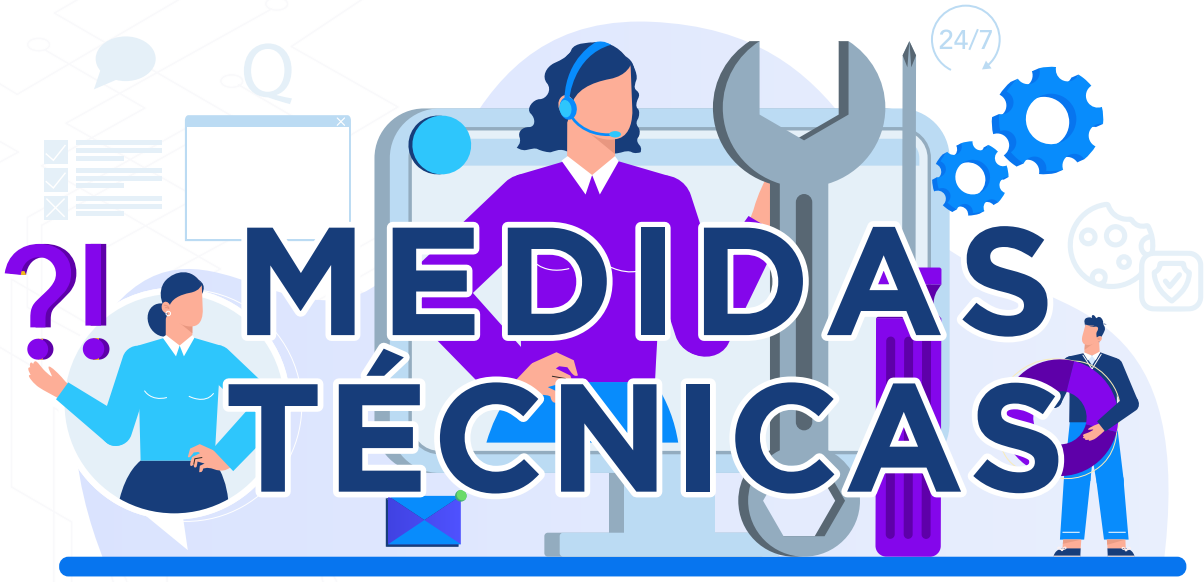
Cookies de sessão ou temporários:

São utilizados enquanto o usuário faz a navegação. Desse modo, quando o usuário encerra a página, desliga o computador, ou quando conclui o serviço que estava utilizando, as informações colhidas são descartadas. Um exemplo clássico são as listas de produtos que são inseridas no carrinho e depois da finalidade escolhida pelo usuário ela é descartada.

Cookies persistentes

O Controlador utiliza esses cookies com objetivo de lembrar as preferências dos usuários. Ele define ainda o tempo em que os dados coletados serão acessados e armazenados. Nessa situação, os dados podem ficar armazenados por anos. A escolha é feita de acordo com a necessidade e finalidade dos dados tratados.

Os sites devem demonstrar de forma clara, visível e acessível o pedido de consentimento para coleta das informações, mesmo sendo apenas o uso de cookie de sessão. Essa autorização pode ser realizada através de um "opt-in" (expressão da vontade de um usuário de Internet ou mobile, afastando-se sua presunção de aceite pelo silêncio).



26 - O QUE SERIA ADOÇÃO DE MEDIDAS TÉCNICAS E ADMINISTRATIVAS PARA AS EMPRESAS?

No cenário atual, em que as atividades econômicas são movidas a dados, é necessária a adoção de estratégias de proteção e segurança de dados, assim como de qualquer outro ativo da empresa, para evitar o risco de perdas financeiras.

A adequação e implementação da LGPD é fundamental. Além das possíveis sanções a serem aplicadas pelos tribunais, incidentes de segurança podem ser fatais para as empresas. Isso porque, não se trata apenas de considerável prejuízo financeiro, pois fato é que a conformidade proteger e evitar máculas à imagem da empresa no mercado, que resultaria na perda de clientes e de credibilidade.
É extremamente importante que as empresas adotem 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.

Nesse sentido, é imperioso perceber que a cada dia os dados, sobretudo aqueles sensíveis, que revelam a esfera íntima das pessoas, adquirem valor próprio e se tornam um ativo ainda mais valioso, por isso merecem maior governança ante penalidades potenciais.
A atividade de adequação às regras da Lei Geral de Proteção de Dados não se resume ao emprego de medidas tecnológicas e padrões de segurança.
Na verdade, inclui, também, a necessidade de elaboração, manutenção e revisão de documentos.

Os artigos 46 e 48 da LGPD, por exemplo, afirmam que:

Art. 46. Os agentes de tratamento 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.
Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Assim, a LGPD deixa clara a responsabilidade dos agentes de tratamento (que são o controlador e o operador) em proteger seus sistemas dos incidentes de segurança de modo preventivo.

Ao nos referirmos a dados pessoais, o maior risco em termos financeiros será quando ocorrer vazamento – ou seja, na possibilidade de exposição dos dados pessoais para terceiros que não têm autorização para ter acesso a eles ou desvio de finalidade de tratamento.

Para evitar isso, cinco medidas são essenciais para garantir a adequação à Lei:

• Utilizar sistema de segurança compatível com os riscos específicos da sua forma de armazená-lo, construído de acordo com as necessidades do seu negócio, que proteja esses dados pessoais e sensíveis;

• Adotar plano de contingenciamento sistêmico e jurídico capaz de abreviar o tempo de enfrentamento e reduzir os danos de eventual vazamento;

• Verificar se os registros eletrônicos gerados pelos sistemas de segurança são capazes de revelar todas as atividades relativas ao tratamento dos dados, de forma que tais informações possam ser acessadas e preservadas como meio de prova. Essas provas poderão ser decisivas num processo judicial oportunamente;

• Dar ampla ciência do incidente aos titulares de dados pessoais envolvidos por meio de comunicação pública, informando quais os dados vazados, o risco de golpes que podem ocorrer a partir desse vazamento, quais medidas jurídicas ou operacionais devem ser adotadas para reduzir o risco.

São exemplos de medidas técnicas:

POLÍTICA DE SENHAS:

- Cada colaborador deve ter sua senha de rede, email e sistemas
- obrigação de logoff após uso do sistema
- alteração periódica das senhas

ANTIVÍRUS

- Adquirir um sistema confiável e robusto
- Mantê-lo atualizado
- Política de restrição de acesso a sites e conteúdos inapropriados e que podem colocar a empresa em risco

BACKUP

- Implantar rotina de backup, preferencialmente na núvem

POLÍTICA DE USO DOS EQUIPAMENTOS ELETRÔNICOS QUAIS DISPOSITIVOS MÓVEIS PODEM OU NÃO SE CONECTAR

- pendrives, hd externos, smarsphones.
- Regular o uso de redes sociais
- Apagar ou copiar arquivos ou informações sem autorização
- Abrir/alterar/manusear hardware da empresa
- Aterar configurações do sistema
- Regular o uso de emails pessoais e corporativos
- Manter os sistemas atualizados

São exemplos de medidas administrativas:

REVISÃO DE CONTRATOS E POLÍTICAS

- Verificar se há políticas, normas, procedimentos relacionados à segurança da informação, armazenamento e descartes de dados, gestão de risco, o que se deve fazer em caso de incidentes como vazamento de dados pessoais;

- Quaisquer outras informações relevantes e específicas para a organização desenvolver um Projeto de Governança Digital.

- Revisar contratos com fornecedores, parceiros, colaboradores, etc.

A LGPD exige a adoção de medidas preventivas para evitar a violação dos direitos fundamentais à privacidade e intimidade dos titulares dos dados pessoais.

Tal imposição deve ser vista como uma possibilidade concedida aos agentes de tratamento e que só traz consequências positivas, em especial considerando-se que a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano decorrente da infração da lei será um item a ser considerado como atenuante no momento de eventual imposição de sanções administrativas.

27 - IMPACTO DA LGPD NAS EMPRESAS (BRASIL)

Ao ser sancionada a Lei Geral de proteção de dados nº 13.709/2018 em agosto de 2018 o Brasil deu um importante passo no sentido de estabelecer regras especiais voltadas à proteção de dados pessoais.

Isso porque, os países que não possuem uma lei específica para tutelar os dados pessoais podem ter o seu desenvolvimento econômico afetado, na medida em que isso implica em perda de oportunidades. Além disso, ainda que o país esteja devidamente regulamentado, as empresas somente conseguem manter-se competitivamente ativas se conseguirem comprovar a efetiva observância das previsões legais.

Para se adequarem às regras estabelecidas pela LGPD e garantir que estejam em conformidade, as empresas devem criar e algumas já estão criando procedimentos operacionais que sejam aplicáveis às suas rotinas diárias, ou seja, elas já estão percebendo a importância, o zelo em cuidar e aplicar a privacidade e proteção de dados em todos os seus processos.

A Lei não visa, de forma alguma, restringir a utilização de dados pessoais para fins econômicos e, em alguns casos, pode-se revelar até mais flexível do que outras legislações setoriais. O que a Lei obriga é que a empresa garanta aos titulares que seus dados pessoais serão tratados com maior transparência, controle e segurança, sob pena de aplicação de sanções severas.

É justamente com enfoque nas medidas de boas práticas e de governança que a LGPD, em seu artigo 50, estabelece que os controladores e operadores, de acordo com suas competências em relação ao tratamento de dados pessoais, poderão formular regras de boas práticas e de governança que definam:

> (...) as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Na prática, o que muda é a forma de tratar os dados pessoais dos associados, que agora se torna obrigação legal, ao contrário das meras boas práticas do passado.

A título de exemplificação, algumas mudanças realizadas pelas empresas após a entrada em vigor da LGPD:

Mudanças no atendimento ao cliente e no marketing, pois todos os dados pessoais alheios precisarão ser tratados de forma a manter a conformidade com a nova legislação.

Deverão ser abordados e reavaliados os processos gerenciais relativos ao tratamento de informações dos clientes, readequando os canais de relacionamento e comunicação.

O papel da área jurídica, de tecnologia e de pessoal da empresa será fundamental para eliminar ou mitigar eventuais impactos nos seus negócios.

A LGPD é um grande marco na utilização mais adequada de informações: com receio das tratativas punitivas, os empreendedores terão processos mais bem organizados e usarão ferramentas e soluções específicas para garantir a segurança da informação em âmbito organizacional.

Via de consequência, a adoção dessas medidas traz uma maior segurança para os demais processos, que não se relacionam ao uso e o tratamento de dados, pois, passam a ser mais bem estruturados e se beneficiam pelo nível de proteção que toda a empresa estará sujeita.

Aos cidadãos em geral, a LGPD traz mais segurança e garantia para a privacidade de informações, que poderiam ser usadas de forma imprudente e até maliciosa com objetivos comerciais e, ainda, difamatórios.

A grande importância da proteção dessas informações, além da garantia da privacidade de seus detentores, é inibir qualquer forma de discriminação.

28 - MITO OU VERDADE?

ESCANEIE PARA VISUALIZAR O CONTEÚDO EM VIDEO

O CONSENTIMENTO É A PRINCIPAL BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS?

A LGPD tem como fundamento a proteção de direitos e garantias fundamentais. Nesse contexto, para a regularidade do tratamento de qualquer dado pessoal, deverá haver o enquadramento em uma das bases legais previstas no art. 7º da LGPD.

Uma dessas bases é o consentimento que, segundo o art. 5º, XII da LGPD, consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Considerando a finalidade da LGPD e o conceito legal do consentimento, há uma tendência de se dar destaque a essa base legal. Mas esse destaque se justifica?

O consentimento é a principal base legal para o tratamento de dados pessoais?
O consentimento é uma das dez bases legais previstas no art. 7, da LGPD para o tratamento de dados pessoais. Dessa forma, não há qualquer hierarquia entre as bases legais.

Por cautela, devemos sempre obter o consentimento do titular do dado pessoal, mesmo quando existem outras bases legais para o tratamento do dado?
Considerando que o titular do dado pessoal poderá revogar o consentimento a qualquer momento, não é recomendável obtê-lo quando houver outra base legal adequada à natureza do tratamento.

Ademais, para um consentimento ser considerado válido, é preciso que ele seja:

- livre,
- informado,
- inequívoco e,
- para finalidade determinada.

Exemplos práticos:

1 - Se a pessoa fornecer o seu CPF para participar de uma promoção por tempo determinado, findo aquele prazo, o dado deverá ser excluído e não poderá ser mais utilizado, pois o consentimento foi dado para uma finalidade específica.

2 - Se você faz o download de um aplicativo e, apesar de não ser essencial para a sua utilização, ele lhe pede acesso à sua localização ou à sua galeria de fotos, obrigatoriamente este aplicativo deverá obter o seu consentimento e lhe informar a finalidade desse tratamento.

Portanto, o consentimento genérico, vago e sem observância dos requisitos acima, será nulo nos termos do art. 8º, §4º da LGPD. E, mesmo com o consentimento do titular, deverão ser observados os princípios previstos na LGPD, em especial, o da transparência, da necessidade, da finalidade e da adequação.

29 - O QUE POSSO E NÃO POSSO FAZER COMO EMPRESA?

Os empresários precisam estar atentos aos menores detalhes da sua organização e da vida de seus colaboradores e fornecedores sobre assuntos societários, financeiros, negócios e outros mais.

Nessas atividades, a empresa deve resguardar o sigilo. A ética profissional é uma questão de sobrevivência. Qualquer empresa é um grande depósito de informações sensíveis e de grande valor, seja nos e-mails trocados internamente pelos sócios, seja na documentação arquivada: detalhes sobre a esfera privada de clientes e colaboradores, patentes, contratos comerciais, preços e valores.

A partir de agora, é obrigação das entidades que o tratamento de dados pessoais sempre ocorra da forma mais segura possível – ou seja, usando normas procedimentais previstas na Lei, como adequar contratos de prestação de serviços com fornecedores, revisar processos internos e externos para evitar os riscos de compartilhamento não autorizado com desvio da finalidade consentida pelo titular.

Para mitigar ou garantir o risco da privacidade dos clientes, um mecanismo que pode ser usado é a anonimização total ou parcial dos dados que identificam o titular. Outra opção é a pseudonimização, que significa a substituição dos dados pessoais que revelam a identidade do titular por outra fictícia.

É importante ter cuidado para que, no ambiente de trabalho, somente tenham acesso aos dados pessoais aqueles que de fato precisam tê-los, respeitando a finalidade do tratamento consentido pelo titular. Essa medida visa evitar casos de negligência ou vazamento proposital que possam vir a ocorrer.

A segurança nos dados passa a ser uma obrigação expressa da Lei, sujeita a penalidades. Por esse motivo, é mandatório que os gestores da organização exerçam a Governança Digital, ou seja, conheçam os riscos envolvidos, enxerguem as lacunas atuais e executem as medidas corretivas.

O quadro abaixo traz alguns exemplos do que as empresas podem e não podem fazer:

PODE	NÃO PODE
Criar ou revisar a forma pelo qual o colaborador ou cliente vai consentir e tomar ciência da finalidade do tratamento de seus dados pessoais, assegurando a possibilidade da revogação desse consentimento futuramente.	Comprar listas de dados: Apesar de parecer uma opção "facilitada" para empreendedores que desejam começar ou alavancar seus negócios, a compra de dados é uma das principais infrações que a LGPD quer barrar. A teor do art. 7º, da LGPD, o legislador estabeleceu dez bases legais para o tratamento de dados, a principal delas é o consentimento do titular. Ou seja, é necessária autorização prévia para que possa ser feito qualquer contato com este indivíduo.
Adotar medidas de proteção dos dados: contar com a consultoria de especialistas para montar um plano de contingenciamento de segurança digital e medidas legais para abreviar o tempo de resposta ao incidente, reduzindo o alcance dos riscos e prejuízos financeiros.	Compartilhar dados: Se a compra de dados é proibida, a venda e compartilhamento sem consentimento, também. Todo terceiro que tratar dados pessoais também será alvo de conformidade no tocante à LGPD. Daí é necessário que este esteja em conformidade quanto a implantar recursos sistêmicos de segurança cibernética, além de se sujeitar às obrigações legais em relação à atividade de tratamento de dados pessoais, sob pena de sanções pesadas.
Criar um canal de comunicação que permita ao titular dos dados a ciência, a alteração ou a revogação do seu consentimento para tratamento de seus dados pessoais.	Entrar em contato com o consumidor sem o seu consentimento.
Tornar anônimos ou pseudônimos os dados pessoais compartilhados com terceiros, se possível, como medida de reduzir o risco.	Coletar dados irrelevantes: Somente colha dados pessoais que a empresa realmente irá utilizar.
Capacitar os colaboradores quanto à segurança da informação e proteção de dados, exemplificando os riscos legais e as medidas procedimentais que serão implantadas.	Utilizar dados para outras finalidades: Ainda que a empresa tenha coletado dados com autorização do consumidor, não é permitido utilizar estas informações para outras finalidades que não foram autorizadas.
Manter-se atualizado quanto às melhores práticas operacionais para o tratamento dos dados pessoais de terceiros.	

O trabalho é complexo apurar lacunas quanto ao tratamento de dados na empresa exige esforço e sensibilização de várias lideranças da empresa, eventos para coleta, análise e revisão dos dados pessoais e das medidas corretivas.

Será necessário que o enfrentamento dessas lacunas seja conduzido por várias pessoas, lideradas por alguém que tenha poder decisório. Não é uma tarefa fácil. As mudanças são necessárias e os empresários têm de estar envolvidos nesse assunto, pois, caso contrário, os prejuízos serão percebidos apenas quando acontecer incidentes futuros.

30 - O QUE POSSO E O QUE NÃO POSSO FAZER ENQUANTO COLABORADOR/EMPREGADO DE UMA EMPRESA, NA QUALIDADE DE TITULAR DOS DADOS?

O empregado contratado por uma empresa possui direitos enquanto titular de dados pessoais e dados pessoais sensíveis, posto que o compartilhamento destas informações junto ao empregador é condição imprescindível para a concretização do vínculo empregatício.

Todavia, enquanto colaborador de uma empresa, este mesmo empregado possui deveres no que concerne ao tratamento de dados pessoais de outros colegas, clientes, terceiros, fornecedores, parceiros, entre outros.

Abaixo, encontram-se elencados exemplos do que pode e o que não pode ser feito pelo EMPREGADO, enquanto Colaborador de uma empresa, no que concerne aos seus direitos e deveres:

O QUE PODE SER FEITO	O QUE NÃO PODE SER FEITO
Ter o livre acesso sobre a utilização dos meus dados pessoais pela empresa e a finalidade correspondente.	Negar a informar dados imprescindíveis à formação regular do vínculo empregatício, tais como nome completo, CPF, carteira de identidade, endereço, nº PIS, dados bancários para pagamentos.
Retificar/ corrigir os meus dados pessoais incorretos.	Negar a realizar o exame médico admissional.
Atualizar os meus dados pessoais, em caso de modificação. Mudança no estado civil e no endereço, por exemplo.	Assinar documentos sem consciência de sua finalidade e conteúdo.
Ter os meus dados pessoais tratados/ utilizados, nos limites necessários para a finalidade laboral.	Deixar de seguir as políticas internas da empresa.
Ler e seguir todos os contratos, termos e comunicados sobre privacidade e proteção de dados pessoais.	Deixar documentos que contenham dados pessoais à mostra, em impressoras, fax, copiadoras, ou na sua mesa de trabalho, de modo a expor a informação.

Tratar os dados pessoais nos limites e finalidades solicitadas pelo meu empregador ou de terceiros. Mas sempre orientado pelo empregador.	Compartilhar senhas utilizadas para o trabalho, como as de e-mail e login de sistemas.
Se recusar a fornecer, ter os dados pessoais tratados, para finalidades adicionais, como receber brindes da empresa, por exemplo.	Utilizar as senhas fornecidas pela empresa, com finalidade profissional, de outro colega de trabalho.
Ler os avisos de cookies e os avisos/ políticas ao acessar os sites.	Compartilhar dados de clientes, fornecedores e colegas de trabalho com terceiros.
Realizar troca periódica de senha.	Compartilhar dados de clientes e fornecedores com colegas de trabalho de forma desnecessária.
Descartar papéis, documentos, que contenham dados pessoais da forma correta, através de uma fragmentadora de papéis (de acordo com as normas da empresa).	Tirar fotos de documentos de clientes e fornecedores.
Ser um agente ativo na diminuição quantos aos riscos relacionados à segurança da informação, dentro e fora da empresa.	Clicar em links enviados por terceiros, sem orientação do empregador.
Ao tomar ciência de uma falha de segurança ou violação à LGPD, reportar imediatamente ao setor competente.	Não baixar qualquer atualização em sistemas sem a recomendação do empregador.
Zelar pela integridade dos dados tratados.	Não expor os colegas de trabalho em grupos de WhatsApp.
Armazenar os dados corretamente, da forma como solicitado.	Solicitar dados para clientes, em quantidade superior à estipulada pelo empregador.
Fazer cursos voltados para privacidade e segurança dos dados.	Tratar dados pessoais de crianças ou adolescentes sem o consentimento dos pais ou responsável.
Manter sigilo sobre dados pessoais de clientes, colaboradores e parceiros, principalmente no que concerne aos dados pessoais sensíveis, tais como, dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa.	Deixar a tela do computador aberta/ exposta, enquanto ausente da estação de trabalho.
	Deixar VPN conectado após encerradas as atividades laborais.
	Acessar redes sociais nos dispositivos móveis da empresa.

Utilizar papéis/folhas que contenham dados pessoais de clientes, colaboradores, fornecedores ou outros colegas como rascunho.

Tratamento discriminatório, considerando a ciência sobre dados pessoais de cliente, colaborador, parceiro, tais como a orientação sexual, escolha religiosa, dentre outros.

Fornecer dados pessoais por e-mail, telefone ou qualquer outro canal inapropriado.

Compartilhar dados pessoais quando solicitado por terceiros que se identificam como autoridade, ou algum colaborador, sem verificar a segurança daquele compartilhamento. Atualmente, existem golpes relacionados a este tipo de manobra.

Expor dados pessoais de clientes, parceiros, fornecedores em redes sociais.

Para acessos fora do ambiente da empresa, principalmente para os colaboradores em home office, evitar utilizar computadores desconhecidos para acessar os sistemas/ e-mails corporativos.

Logar com os dispositivos móveis da empresa em redes wifi pública.

A tabela acima exposta contém orientações básicas e primordiais para todo aquele que se enquadra na condição de empregado/colaborador de uma empresa.

Porém, o que a lei pretende com suas disposições, é promover uma mudança de consciência dos cidadãos, sobre a importância de serem adotados cuidados quando o assunto é tratamento de dados pessoais próprios e de terceiros.

Tendo em mente a importância de resguardar os dados pessoais e compartilhá-los apenas nos limites e para que sejam cumpridas as finalidades necessárias, cada cidadão possui em si o potencial para ser um agente transformador no que concerne à cultura da proteção de dados.

REFERÊNCIAS

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Revista dos Tribunais, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 06 de outubro de 2022.

BRASIL. Ministério da Cidadania. Acesso à informação, 2022. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em: 06 de outubro de 2022.

BRASIL. GOVERNO DIGITAL. Guia de boas práticas Lei Geral de Proteção de Dados (LGPD). Abr. 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf> Acesso em: 06 de outubro de 2022.

BRASIL. Ministério da Economia. Governo Digital, 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>. Acesso em: 06 de outubro de 2022.

Melhores práticas de Governança e Conformidade com a LGPD. Opiceblumacademy Opice. Disponível em: <https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf >. Acesso em: 11 out. 2022.

Cadernos de Direito Empresarial, 15ª Vol, 2020, Gaia Silva e Gaede Advogados
https://opiceblum.com.br/ebooks/
Lei nº 13.709/2018 (LGPD)

CAMPELLO, Marcos André Barbosa; GUIMARÃES, Daniel Miaja Simões; JUNIOR, Antônio Araújo; MENEZES, Aline; VILELA, Camila Maria de Moura. O que estão fazendo com meus dados? A importância da Lei Geral de Proteção de Dados. Pernambuco: OAB Pernambuco. E-book. Disponível em: <https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf> Acesso em: 03 out. 2022.

CRESPO, Marcelo. Compliance Digital. In: NOHARA, Irene Patrícia; PEREIRA, Flávio de Leão Bastos. Governança, compliance e cidadania. 2ª ed. São Paulo: homson Reuters Brasil, 2019. Edição Kindle. Posição 5405.

DA SILVA, Alexandre Pacheco (org.). Guia de Proteção de Dados Pessoais – Transferência Internacional. FGV, 2020. Disponível em: <https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf> Acesso em: 06/10/2022.

E-book: Melhores práticas de Governança e Conformidade com a LGPD. OpiceBlum. Disponível em: <https://28563dcd-7409-4c91-96aa-c236d9f0a871.usrfiles.com/ugd/28563d_6971dd5b77484c2c9d0c26388a324cf6.pdf> Acesso em: 17 out. 2022.

Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018: doutrina e aplicabilidade no âmbito laboral [recurso eletrônico] / organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022. 685 p.; PDF; 6MB. ISBN: 978-65-995463-8-9 (Ebook) Direito. 2. Direito digital. 3. Lei Geral de Proteção de Dados. I. Barzotto, Luciane Cardoso. II. Costa, Ricardo Hofmeister de Almeida Martins. II. Título. III. Brasil. Tribunal Regional do Trabalho (4ª Região) Escola Judicial do Tribunal Regional do Trabalho da 4ª Região
Giarllarielli advogados. Direitos do titular de dados – LGPD. Disponível em: <https://www.giarllarielli.adv.br/direitos-do-titular-de-dados-lgpd/>. Acesso em: 05 out. 2022.

HOLLANDA, Bernardo Buarque de. No tempo do futebol-arte. Revista História da Biblioteca nacional, Rio de Janeiro, ano 9, n. 105, p. 58-59, jun. 2014. p. 58.

JUNIOR, Irineu Francisco Barreto; NASPOLINI, Samyra Haydêe Dal Farra. Proteção de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro: Stamppa, 2019. 160 p. KATEIFIDES, Alexis; BATES, Joel; PAPAGEORGIOU, Nikos; RAMSEY, Rumer; VAN DER GEEST, Bart; MARINI, Alice; ARGUINARENA, Pascale; ASHCROFT, Victoria. Comparing privacy laws: GDPR vs. LGPD. OneTrust. 2020. 56 p.

Lei Geral de Proteção de Dados Pessoais (LGPD). SwisscamBrasil. Disponível em: <https://swisscam.com.br/publicacao/doing-business-in-brazil/33-lei-geral-de-protecao-de-dados-pessoais-lgpd/> Acesso em: 17 out. 2022.

LGPD: conheça seus direitos como titular de dados pessoais. Mittechreview. Disponível em: <https://mittechreview.com.br/lgpd-conheca-seus-direitos-como-titular-de-dados-pessoais/>. Acesso em: 05 out. 2022.

Lima, Ana Paula Moraes Canto de. LGPD – Lei Geral de Proteção de Dados (recurso eletrônico): sua empresa está pronta? / Ana Paula Moraes Canto de Lima, Dionice de Almeida, Eduardo Pereira Maroso– São Paulo, SP: Literante Books International, 2020.

LIMA, José Jerônimo Nogueira De. A Estruturação da Autoridade Nacional de Proteção de Dados: Desafios para a Efetividade da LGPD. Conteúdo Jurídico. p. 25.

MONTEIRO, Yasmin Sousa. A efetividade dos mecanismos de proteção de dados pessoais na lei 13.709/2018. 2019. Monografia (Bacharel em Direito) - Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB), Brasília, 2019.

O que acontece quando você aceita os cookies de um site e por que é bom apagá-los de tempos em tempos. BBC. Disponível em: <https://www.bbc.com/portuguese/geral-40730996>. Acesso em: 13 de outubro. 2022.

O que é e como elaborar o Relatório de Impacto à Proteção de Dados Pessoais. Getprivacy. Disponível em: <https://getprivacy.com.br/relatorio-de-impacto-lgpd/>. Acesso em: 17 out. 2022.

Pedrosa, Clara Bonaparte. Direito E Tecnologia: Discussões Para o Século XXI, Erechim: Ed Deviant Ltda, 2020. 190 p.

Pohlmann, Sérgio Antônio. LGPD Ninja Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas o qual detém todos os direitos autorais sobre ele, sob número 312235936 timestamp 2019-08- 06 11:37:18 GMT. Editora Fross

Quais os Direitos dos Titulares de Dados Pessoais na LGPD? Tenbu. 2021. Disponível em <https://www.tenbu.com.br/quais-os-direitos-dos-titulares-de-dados-pessoais-na-lgpd-2/>. Acesso em: 05 out. 2022.

RAFAEL, Luana Galetti; SANTOS, Gabriel Teixeira. A advocacia e a proteção de dados na revolução industrial do século XXI. ETIC 2018 - Encontro de Iniciação Científica.

SANTOS, Alexandre da Silva. A Importância da Atuação da Auditoria Interna na Implementação da Lei Geral de Proteção de Dados nas Empresas Públicas. 2019. Dissertação (Mestrado Profissional Em Gestão e Políticas Públicas) - Fundação Getúlio Vargas Escola de Administração de Empresas de São Paulo. São Paulo, 2019.

SHIMABUKURO, Rafael Mitsuo Suyama. A responsabilidade civil na nova lei geral de proteção de dados pessoais. 2019. Monografia (Bacharel em Direito) - Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente. Presidente Prudente, 2019.

VAINZOF, Rony. Capítulo I, Disposições Preliminares. LGPD: Lei Geral de Proteção de Dados Pessoais comentada. Ed. 2022. Revista dos Tribunais. Lei nº 13.709 de 14 de agosto de 2018. Capítulo I, Disposições Preliminares, art. 5º, Página RL- 1.2. Acesso em:<https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.2>

GLOSSÁRIO

Para apreender e se divertir quando estiver com dúvida!

Adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao titular, conforme o contexto do tratamento;
Agentes de tratamento: o controlador e o operador;
Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a empresa;
ANPD: Órgão da administração pública direta federal com atribuições relacionadas à regulamentação e fiscalização do cumprimento da LGPD;
Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Colaborador: pessoa natural que faz parte do quadro Colaborador da Organização.
Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Encarregado(DPO): 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);
Finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
Livre acesso: é a garantia dada aos titulares a consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;
Necessidade: o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
Parceiro/Prestador Parceiro: Pessoa natural ou jurídica que prestar serviços a empresa no âmbito das atividades;
Responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.
Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;