# *eBook* de Conscientização sobre a LGPD

Lei Geral de Proteção de Dados Pessoais

every
CYBERSECURITY GRC PRIVACY

UN GLOBAL COMPACT

CERTIFICADA ISO 27001 SEGURANÇA DA INFORMAÇÃO

CERTIFICADA ISO 27701 PRIVACIDADE DA INFORMAÇÃO

# Sumário

# 01 Introdução

O *eBook* de Conscientização sobre a LGPD objetiva auxiliar na compreensão, promoção e disseminação da cultura de privacidade, a fim de viabilizar a observância e a aplicação da LGPD no processo de tratamento de dados pessoais.

A partir dos conceitos abordados ao longo deste *eBook*, será possível constatar que o compromisso com a privacidade é responsabilidade de todos nós!

Este *eBook* apresenta, de forma didática e objetiva, os conceitos e as informações referentes à privacidade e à proteção de dados pessoais.


Nesse sentido, são abordados os seguintes aspectos: explicações sobre os atores envolvidos no tratamento de dados, como titular, operador e controlador, as hipóteses legais que autorizam o tratamento de dados, os direitos dos titulares, bem como temas relacionados às diretrizes da LGPD, ANPD e demais órgãos competentes.

# 02 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), entrou em vigor em 18 de setembro de 2020 para regulamentar o tratamento de dados pessoais nos meios físicos e digitais, por toda e qualquer pessoa física ou jurídica, que realize a coleta e o tratamento de dados pessoais em território nacional, bem como para fins de fornecimento de bens ou serviços, nos termos do art. 3º da referida legislação.

# 03 Conceitos e Definições

Para compreender melhor a LGPD, constam, abaixo, os principais conceitos e definições relacionados à Lei:

**Dados Pessoais**

Qualquer informação que possa identificar ou tornar identificável a pessoa natural (art. 5º, I da LGPD). Exemplo: nome, CPF, RG, dados bancários, profissão, nacionalidade, endereço, localização etc.

**Dados Pessoais Sensíveis**

Nos termos do art. 5º, II da LGPD, "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".

Em outras palavras, quando há a coleta desse tipo dado, faz-se necessário adotar mecanismos de segurança mais eficazes.

## Tratamento de Dados Pessoais

"Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

A título de exemplo, o simples acesso a um dado pessoal em uma tela de computador já caracteriza o tratamento de dado pessoal.

## Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V da LGPD). É importante reforçar que a LGPD não inclui dados de pessoas jurídicas. Exemplo: CPF é um dado pessoal, CNPJ não.

## Operador

Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII da LGPD). Exemplo: empresas terceirizadas que realizam o tratamento de dados pessoais em nome da Instituição.

## Controlador

Pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais (art. 5º, VI da LGPD). Exemplo: A Every Cybersecurity and GRC Solutions.
Observação: De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), "não são considerados controladores os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento".

## Encarregado (Data Protection Officer -DPO)

O Encarregado é a 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 (art. 5º, VIII da LGPD).

Em caso de dúvidas relacionadas ao tratamento de dados pessoais, entre em contato com o nosso DPO pelo e-mail: encarregado@every.com.br ou diretamente no Portal Fale com o DPO.

## Autoridade Nacional de Proteção de Dados (ANPD)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, além de possuir atribuições relacionadas à proteção de dados pessoais e à privacidade em todo o território nacional (art. 5º, XIX).

# 04 Importância da proteção dos dados pessoais

Para que uma instituição mantenha sua integridade e possa se desenvolver de forma saudável, a segurança de dados pessoais deve ser considerada prioridade.

Assim, entende-se que a ausência de conformidade com a LGPD pode acarretar prejuízos que vão desde a perda de confiança devido à publicização de incidentes com dados pessoais até sanções ainda mais graves.

Para tanto, os agentes deverão garantir que os tratamentos de dados pessoais possuam finalidade específica, com base em hipótese legal e com observância às demais diretrizes da LGPD.

# 05 Bases legais e hipóteses de tratamento

Para garantir o tratamento regular dos dados pessoais, além de ser coletado para finalidade específica, esse deve ser fundamentado em uma ou mais hipóteses previstas no art. 7º e 11 da LGPD.

O tratamento de dados pessoais poderá ser realizado apenas nas seguintes hipóteses:

a) Mediante o fornecimento de consentimento pelo titular;

b) Para o cumprimento de obrigação legal ou regulatória pelo controlador;

c) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

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

e) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular, a pedido do titular dos dados;

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

**g)** Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

**h)** Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

**i)** Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

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

Já o tratamento de dados pessoais sensíveis poderá ser realizado somente: (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 legais definidas no art. 7º, afastado o Legítimo Interesse.

# 06 Exercícios de direitos pelos titulares

A proteção dos dados pessoais é um direito fundamental, disposto no art. 5º da Constituição Federal, e deve ser exercido por todo e qualquer titular. Nesse sentido, inclui-se:

a) **Confirmação** da existência de tratamento;
b) **Acesso** aos dados;
c) **Correção** de dados incompletos, inexatos ou desatualizados;
d) **Anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
e) **Portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
f) **Eliminação** dos dados pessoais tratados com o consentimento do titular, **exceto** nas hipóteses previstas no art. 16 da LGPD;
g) **Informação** das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h) **Informação** sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
i) **Revogação do consentimento,** quando os dados estivem sendo tratados com base nesse fundamento.


É importante destacar que as solicitações deverão ser recebidas de forma gratuita e em observância ao prazo de até 15 (quinze) dias para atendimento pelo Encarregado (em inglês, Data Protection Officer – DPO), salvo quando legislação específica defina um prazo distinto, como no caso de tratamento de dados pessoais realizado pela Administração Pública.

Para exercícios dos direitos previstos na LGPD, os controladores devem disponibilizar um canal de contato entre os titulares e o Encarregado.

# 07 Sanções administrativas

Em caso de descumprimento da LGPD, poderão ser aplicadas sanções, com base na análise do caso concreto e gravidade do dano aos titulares, conforme Regulamento de Dosimetria e Aplicação de Sanções Administrativas estabelecido pela ANPD.

a) Advertência;

b) Multa simples, de até 2% do faturamento da pessoa jurídica, limitado a R$ 50.000.000,00 (cinquenta milhões) por infração;

c) Multa diária;

d) Publicização da infração;

e) Bloqueio dos dados pessoais;

f) Eliminação dos dados pessoais;

g) Suspensão parcial do funcionamento do banco de dados pelo período máximo de 6 meses, prorrogáveis por igual período;

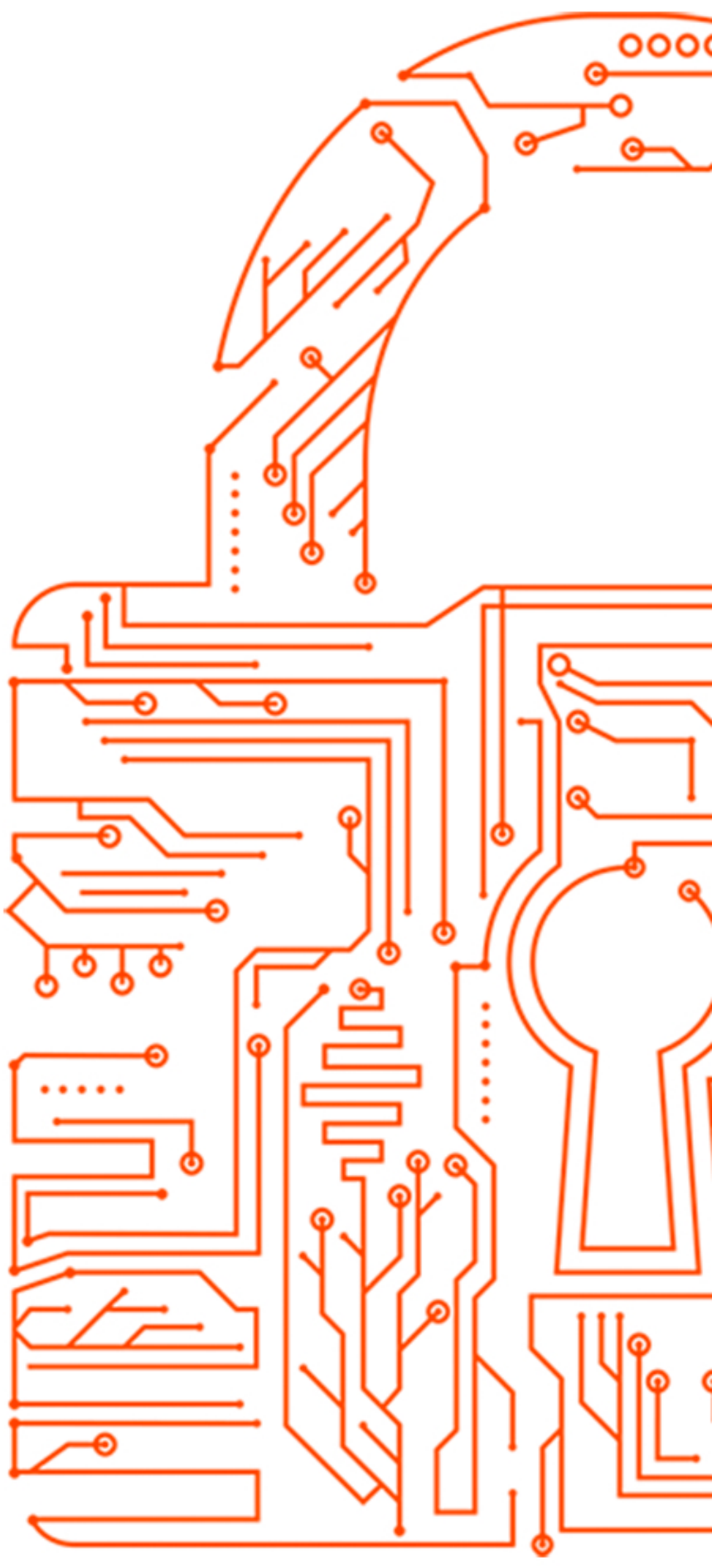
h) Suspensão do exercício da atividade de tratamento dos dados pessoais pelo período máximo de 6 meses, prorrogáveis por igual período; e

i) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

# 08 Medidas técnicas e administrativas de segurança

Com o propósito de preservar a segurança dos dados pessoais e, por consequência, mitigar riscos de aplicação de sanções pela ANPD, os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais (art. 6º, inciso VII da LGPD).

As medidas devem ser aplicadas tanto nos ambientes físicos quanto digitais em que há o tratamento de dados pessoais. Tendo em vista o caráter principiológico da LGPD, é fundamental observar normas complementares que materializem a conformidade das organizações à legislação vigente, como a ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701.



# 09 Gestão de contratos e a LGPD

Em casos de compartilhamento ou contratação de empresas terceirizadas, é importante zelar pela confidencialidade e pela privacidade dos dados pessoais compartilhados entre a instituição e as empresas.

Nos casos de compartilhamento ou contratação de terceirizadas, é importante zelar pela **Confidencialidade** e **Privacidade** dos dados pessoais compartilhados entre a Instituição e as empresas.

Para manter a conformidade com a proteção dos dados pessoais tratados quando houver relação contratual das organizações com outras empresas, faz-se necessário:

Haja **adequação contratual**, para assegurar que ambas as partes do contrato compreendem a importância do devido tratamento de dados pessoais;

Sejam atendidos os princípios da **finalidade** (propósitos legítimos) e **coleta mínima**; e

Notificar imediatamente possíveis **incidentes** para a outra parte do contrato e ao respectivo Encarregado.

# 10 Violação de Dados Pessoais

Incidentes de segurança são eventos indesejados ou inesperados que possuem grande probabilidade de comprometer as operações e ameaçar a segurança da informação. A título de exemplo, um incidente pode causar interrupção do serviço ou redução da sua qualidade.

Em caso de incidentes envolvendo dados pessoais, poderá ocorrer a destruição, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais, que podem representar risco ou dano relevante para o titular. Por isso, deverão ser tratados de forma conjunta pela equipe de Segurança da Informação e o Encarregado de Dados (DPO).

Caso seja identificado um alto risco de dano aos titulares, as violações de dados deverão ser comunicadas tanto à ANPD quanto aos titulares pelo controlador ou Encarregado, no prazo de até 02 (dois) dias úteis, a fim de que esses tenham ciência do ocorrido e possuam um prazo razoável para atuarem contra o vazamento de dados.

O objetivo do procedimento de resposta a incidentes é minimizar os danos que poderiam ser causados pela violação de dados pessoais, bem como reduzir o tempo de ação e os custos de recuperação.

Em apoio ao Encarregado de Dados (DPO), aqueles que identificam o incidente têm papel fundamental na comunicação e colaboração do tratamento de incidentes que possam gerar danos aos titulares de dados pessoais.

**Lembrando: O compromisso com a privacidade é responsabilidade de todos nós!**

TODOS que se relacionam em algum momento com as organizações e realizam tratamento de dados pessoais devem zelar pela PRIVACIDADE na execução das atividades, bem como pela conscientização daqueles que possuam acesso a dados pessoais, a fim de evitar a não conformidade com a LGPD.

# 11 Privacidade e a Concepção por padrão

Para garantir a privacidade dos titulares e a adequação da proteção dos dados pessoais, é fundamental realizar atividades desde a concepção até a conclusão do tratamento.

A privacidade, desde a concepção (em inglês, privacy by design), possui como objetivo analisar possíveis problemas na tratativa dos dados pessoais e atuar de forma preventiva, antes que incidentes aconteçam. Assim, a privacidade deve ser considerada por padrão e incorporada aos valores e objetivos estratégicos das organizações.

Abaixo, constam os 7 pilares do Privacy by Design, uma das principais formas de implementar, na prática, a privacidade e a proteção de dados pessoais:

**1. Ser proativo e não reativo** – Prevenir e não remediar

Deve haver o monitoramento constante das atividades, análise de riscos e desenvolvimento de correções sempre que uma vulnerabilidade for identificada;

**2. Privacidade por padrão**

Proporcionar a máxima proteção ao usuário, de forma contínua;

**3. Privacidade incorporada ao design**

A privacidade não deve ser vista como um complemento ao projeto, visto que ela é a parte intrínseca e indissociável;

**4. Funcionalidade completa** - Soma positiva, ao invés de soma zero

A proteção dos dados pessoais deve beneficiar todas as partes envolvidas no tratamento;

**5. Segurança de ponta a ponta**

Os dados devem seguir seu fluxo de forma segura, desde o início até sua destinação, de forma que não sejam esquecidos e arquivados de maneira indiscriminada;

## 6. Visibilidade e transparência

Os agentes de tratamento devem prezar pelo completo atendimento dos direitos dos titulares, oferecendo meios de comunicação para possíveis solicitações;

## 7. Respeito pela privacidade do titular

As atividades devem ser centradas na privacidade do usuário, atentando-se à proteção completa dos dados pessoais.

Para assegurar que o tratamento dos dados pessoais não ocorra de modo irregular ou resulte em danos relevantes aos titulares, faz-se necessário adotar medidas técnicas e administrativas, desde a concepção até a conclusão de produtos ou serviços que tratem dados pessoais.

# 12 Agentes de Tratamento

Nos termos da LGPD, o controlador é responsável por tomar decisões relacionadas ao tratamento de dados pessoais, bem como direcionar os operadores acerca do uso, manutenção e armazenamento das informações.

A função do operador pode ser exercida por fontes externas à instituição, como empresas terceirizadas, as quais ficam responsáveis por executar as atividades conforme orientações do controlador.

# 13 Responsabilidade dos agentes

Tanto o controlador como o operador podem ser responsabilizados pelo tratamento indevido dos dados pessoais que causem danos patrimoniais, morais, individuais ou coletivos aos titulares (art. 42). — hipótese em que esse responderá conjuntamente com o controlador (art. 42, §1º, I).

Além disso, caso haja envolvimento de diversos controladores, esses responderão solidariamente entre si, quando atuarem em tratamento de dados pessoais que resultem em dano aos titulares — salvo casos previstos no art. 43 da LGPD (art. 42, §1º, II).

Abaixo, constam alguns fatos que podem acarretar a responsabilidade civil:

a) Vazamentos (data leaks);

b) Não atendimento aos direitos do titular; e

c) Tratamento em desconformidade com a LGPD.

Para mitigar a ocorrência desses riscos, é importante que todas as partes que tratam dados pessoais observem as diretrizes da LGPD, bem como orientações internas das organizações, a fim de resguardar a privacidade dos titulares.

Great Place To Work.®
Certificado
Dez/2022 - Dez/2023
BRASIL

CERTIFICADA ISO
27001
27701

# every

## CYBERSECURITY AND GRC

every.com.br (61) 3548-1994 everycybersecurity contato@every.com.br