



PROTEÇÃO DE DADOS NO BRASIL

DIRETRIZES
PARA EMPRESAS
ESTRANGEIRAS



1	A quem se aplica a LGPD?	3
2	Se a empresa está adequada ao GDPR, automaticamente estará LGPD?	3
3	Quem fiscaliza o cumprimento da LGPD no brasil?	4
4	Agentes de Tratamento	4
5	Encarregado pelo Tratamento de Dados Pessoais (DPO)	5
6	Requisitos para o Tratamento de Dados Pessoais no Brasil	5
7	E se a LGPD não for cumprida?	6
8	Checklist de adequação à LGPD para empresas estrangeiras	7

Proteção de Dados no Brasil

Diretrizes para Empresas Estrangeiras



1 A quem se aplica a LGPD?

A Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou “LGPD”) se aplica a qualquer pessoa natural ou jurídica de direito público ou privado que realize tratamento de dados pessoais: (i) no território brasileiro; (ii) com dados pessoais coletadas no território brasileiro; ou (iii) que tenha por objetivo fornecer bens e/ou serviços aos indivíduos localizados no Brasil, conforme o art. 3º, LGPD.



Empresas localizadas fora do Brasil podem estar sujeitas às regras da LGPD.

2 Se a empresa está adequada ao GDPR, automaticamente estará LGPD?

A adequação ao GDPR representa um avanço relevante para o cumprimento da LGPD, mas não equivale, por si só, à conformidade com a legislação brasileira, uma vez que se tratam de normas distintas, com requisitos próprios, tais como:

TEMA

COMPARATIVO GDPR E LGPD

Bases Legais

A LGPD prevê hipóteses próprias, não presentes no GDPR, que autorizam o tratamento de dados, como a proteção ao crédito e a tutela da saúde.

Crianças e Adolescentes

O GDPR prevê regras para o tratamento de dados pessoais de menores de 16 anos, podendo haver regras específicas previstas pelos Estados-Membros. No Brasil, considera-se criança a pessoa até 12 anos incompletos e adolescente aquela entre 12 e 18 anos de idade.

Transferência Internacional

Enquanto o GDPR regula as transferências internacionais de dados pessoais a partir dos países da Área Econômica Europeia, a empresa submetida à LGPD deve observar as regras específicas aplicáveis às transferências internacionais de dados realizadas a partir do território brasileiro para país estrangeiro ou organismo internacional (Art. 33, LGPD e Resolução Normativa CD/ANPD n.º 19/24).

Encarregado (DPO) e Registros

No GDPR, nomeação de DPO e Registro das Operações de Tratamento (Record of Processing Activities) não é mandatório em todos os casos. Na LGPD, estas são obrigações legais exigidas de todos os controladores, salvo exceções específicas para agentes de pequeno porte.

Proteção de Dados no Brasil

Diretrizes para Empresas Estrangeiras



3 Quem fiscaliza o cumprimento da LGPD no Brasil?

A principal entidade responsável por fiscalizar a proteção de dados pessoais no Brasil é a:

Agência Nacional de Proteção de Dados (ANPD), com poderes para regulamentar, fiscalizar e sancionar em matéria de proteção de dados pessoais.

A ANPD conta com **processos estruturados para apuração de infrações e para aplicação de sanções**.



Outras entidades brasileiras como o PROCON, o Ministério Público e órgãos setoriais, como ANEEL, SUSEP, BACEN, ANS, também podem atuar no tema de proteção de dados pessoais.

4 Agentes de Tratamento

Para regular o tratamento de dados, a LGPD definiu dois agentes de tratamento:

- **Controlador:** pessoa natural ou jurídica a quem compete **tomar decisões sobre elementos essenciais do tratamento** de dados pessoais, como a finalidade, dados a serem tratados e a duração do tratamento.
- **Operador:** pessoa natural ou jurídica que **realiza o tratamento de dados em nome do controlador e conforme as instruções deste**, com poder para decidir sobre os elementos não essenciais do tratamento.

RESPONSABILIDADES DO CONTROLADOR

Responder às requisições de titulares que exercerem seus direitos

Comunicar à ANPD e aos titulares sobre a ocorrência de incidentes

Responsabilizar-se por violações à lei que causar e, solidariamente com o operador, por infrações que este causar

RESPONSABILIDADES DO OPERADOR

Comunicar e/ou obter autorização do controlador caso subcontrate terceiros que atuem no tratamento de dados pessoais

Firmar contratos com o controlador que documentem as atividades de tratamento de dados pessoais e respectivas responsabilidades.

Responsabilizar-se pela inobservância à lei, ao contrato ou as instruções lícitas recebidas do controlador



A ANPD, por meio de guia orientativo, definiu também as figuras do:

- **controlador conjunto:** que define o tratamento junto de outro controlador; e do
- **suboperador:** subcontratado do operador para cumprir instruções do controlador

Proteção de Dados no Brasil

Diretrizes para Empresas Estrangeiras



5 Encarregado pelo Tratamento de Dados Pessoais (DPO)

Conforme as regras da LGPD e as resoluções da ANPD, o controlador deverá nomear um Encarregado.

O Encarregado é indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.



Empresas estrangeiras sujeitas à aplicação da LGPD em razão do tratamento de dados pessoais que realizam, **devem nomear Encarregado para a organização** (salvo se a empresa for considerada agente de pequeno porte, no Resolução CD/ANPD nº 02/2022)

Pontos importantes :

- a nomeação do Encarregado deve ocorrer por ato formal que designe pessoa física ou jurídica capaz de comunicar-se com titulares e ANPD em língua portuguesa e de forma clara; e
- a organização deve garantir que o Encarregado tenha meios e recursos (humanos, técnicos e administrativos) para cumprir suas funções legais, de forma autônoma e independente, sem conflitos de interesse em sua atuação.

6 Requisitos para o Tratamento de Dados Pessoais no Brasil

1. **estabelecimento de finalidade legítima e específica:** o tratamento deve atender a um propósito claro, determinado e que não viole leis brasileiras e/ou direitos por esta protegidos.
2. **adoção de base legal adequada:** o tratamento deve estar respaldado em uma das hipóteses previstas na LGPD que autorizam tal operação. As bases legais variam conforme as características do tratamento e a natureza dos dados pessoais tratados, por exemplo:

PARA DADOS PESSOAIS (ART. 5º, I DA LGPD)

(EX.: NOME, CPF, RG, IDADE, GÊNERO ETC.)

Aplicam-se as bases legais do art. 7º:

- Consentimento
- Cumprimento de Obrigações Legais
- Tutela da Saúde
- Proteção à Vida
- Exercício regular de direitos
- Execução de contratos
- Proteção ao Crédito
- Legítimo Interesse
- Execução de Políticas Públicas
- Estudos por Órgãos de Pesquisa

PARA DADOS PESSOAIS SENSÍVEIS (ART. 5º, II DA LGPD)

(EX.: VIDA SEXUAL, ORIGEM RACIAL, RELIGIÃO, SAÚDE, FILIAÇÃO FILOSÓFICA OU POLÍTICA, GENÉTICO ETC.)

Aplicam-se as bases legais do art. 7º:

- Consentimento
- Cumprimento de Obrigações Legais
- Tutela da Saúde
- Proteção à Vida
- Exercício regular de direitos
- Execução de contratos
- Proteção ao Crédito
- Legítimo Interesse
- Execução de Políticas Públicas
- Estudos por Órgãos de Pesquisa

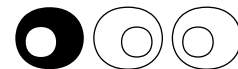
2 Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

3 Resolução CD/ANPD nº 18/2024 - Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

4 Mais informações sobre a nomeação e as funções do Encarregado podem ser encontradas na Resolução CD/ANPD nº 18/2024 e no Guia Orientativo Atuação do encarregado pelo tratamento de dados pessoais publicado pela ANPD em dezembro de 2024.

Proteção de Dados no Brasil

Diretrizes para Empresas Estrangeiras



3. Cumprimento das demais regras da LGPD, com destaque para:

- **Viabilização do exercício dos direitos pelos Titulares de Dados (art. 18, LGPD)**, como a confirmação do tratamento, acesso, correção, eliminação ou bloqueio dos dados, portabilidade, revogação de consentimento, dentre outros.
- **Registro das atividades de tratamento de dados realizadas pela organização (art 37, LGPD).**
- **Elaboração de Teste de Balanceamento, Relatório de Impacto à Proteção de Dados, Avaliação do Melhor Interesse de Menores e procedimentos de Privacy by Design**, quando necessário, nos termos da LGPD, Guias e Resoluções aplicáveis
- **Adotar um dos mecanismos legais (art. 33, LGPD e Resolução CD/ANPD n.º 19/24) para a realização de transferência internacional de dados pessoais**, tomando as providências necessárias para garantir sua validade.

7 E se a LGPD não for cumprida?

Possíveis consequências do descumprimento:

1. Ocorrência de Incidentes de Segurança:

A falta de controles adequados pode gerar acessos não autorizados, divulgação indevida, exposição indesejada ou situação acidental ou intencional de destruição, deleção, perda, alteração envolvendo dados pessoais.

Em caso de incidente:

- Os titulares, terceiros e a própria organização podem sofrer danos;
- Incidentes que causem risco ou dano relevante devem ser comunicados em até 3 dias úteis a ANPD e pessoas afetadas (art. 43, LGPD e Resolução CD/ANPD n.15/24);
- Será necessário adotar medidas para conter o incidente, mitigar danos causados e, ainda, registrar o ocorrido de todo e qualquer incidente, mantendo por no mínimo 5 anos (Resolução CD/ANPD n.15/24)

2. Responsabilização pelas desconformidades legais

Eventual desconformidade pode sujeitar a empresa infratora à (i) responsabilização por danos decorrentes das violações à LGPD e aos direitos de individuais de titulares ou terceiros e (ii) fiscalização e sancionamento pela ANPD, podendo gerar:

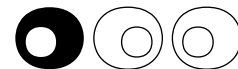
- Obrigação judicial de indenizar os danos causados a pessoas e organizações;
- Imposição de sanções administrativas:

5 O Relatório de Impacto à Proteção de Dados está regulado pelo art. 38 da LGPD e foi alvo de manifestação da ANPD, sendo necessário em casos como a realização de tratamento de alto risco. O Teste de Balanceamento é recomendado para casos de adoção do legítimo interesse como base legal, conforme o Guia Orientativo Hipóteses Legais Legítimo Interesse da ANPD. A Avaliação do Melhor Interesse de Menores e procedimentos de Privacy by Design não foram regulamentados pela ANPD.

6 As regras para realização de transferências internacionais de dados sujeitos à LGPD estão previstas no Capítulo V da LGPD e na Resolução CD/ANPD n.º 19/2024.

Proteção de Dados no Brasil

Diretrizes para Empresas Estrangeiras



- I - Advertência, com indicação de prazo para adoção de medidas corretivas;
- II - 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;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicação da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração; X - 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;
- XI - 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;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

8 Checklist de adequação à LGPD para empresas estrangeiras

Neste sentido, é recomendado a empresas localizadas no exterior:

- ☐ Mapear e registrar atividades de tratamento de dados pessoais sujeitas à LGPD;
- ☐ Identificar a participação da empresa e o fluxo de dados pessoais em cada uma das atividades mapeadas;
- ☐ Analisar o cumprimento dos requisitos de viabilidade para tratamento dos dados (vide item 6 acima);
- ☐ Eleger um Encarregado, observando as regras estabelecidas pela a ANPD na Resolução CD/ANPD n.º18/24 e Guia Orientativo sobre a Atuação do encarregado pelo tratamento de dados pessoais.
- ☐ Ministrar treinamentos periódicos em Proteção de Dados Pessoais para todos os envolvidos, direta e indiretamente, com o tratamento de dados pessoais.
- ☐ Atualizar o Aviso de Privacidade para disponibilizá-lo em língua portuguesa, com as informações exigidas pela LGPD e pelas resoluções da ANPD;
- ☐ Revisar os procedimentos e fluxos de atendimento aos direitos dos titulares para assegurar os prazos e regras da LGPD são cumpridos;
- ☐ Revisar políticas corporativas para que suas previsões estejam em acordo com a LGPD e boas práticas;
- ☐ Revisar contratos com fornecedores e demais parceiros para assegurar que o tratamento realizado com apoio de terceiros está de acordo com as regras brasileiras - especialmente se envolverem transferência internacional;
- ☐ Consolidar e monitorar demais pontos do programa de governança em proteção de dados para assegurar que se alinha à LGPD e diretrizes publicadas pela ANPD e demais órgãos setoriais aplicáveis.

The logo for Opice Blum. The word "Opice" is in a large, bold, white sans-serif font. Below the "ice" part of "Opice", the word "BLUM" is written in a smaller, all-caps, white sans-serif font.

Opice
BLUM

Redefinindo os limites do possível.