

Manual da Lei Geral de Proteção de Dados (Lei 13.709/18)

INDEX

Pag 02	Capítulo 1 LGPD
Pag 03	Capítulo 2 Conceitos chaves
Pag 04	Capítulo 3 princípios
Pag 05	Capítulo 4 Diretos dos titulares
Pag 06	Capítulo 5 Principais obrigações
Pag 07	Capítulo 6 Aplicabilidade passo a passo

Capítulo 1 - LGPD



DA LEI FEDERAL

Após 8 anos de debates e com base no “General Data Protection Regulation”, GDPR, que é o regulamento de Proteção de Dados da União Européia, foi sancionada em 14 de Agosto de 2018 a Lei Geral de Proteção de Dados brasileira.



DA VIGÊNCIA DA LEI

Após 8 anos de debates e com base no “General Data Protection Regulation”, GDPR, que é o regulamento de Proteção de Dados da União Européia, foi sancionada em 14 de Agosto de 2018 a Lei Geral de Proteção de Dados brasileira.



DA ABRANGÊNCIA DA LEI E SUAS SANÇÕES

A Lei tem aplicação extraterritorial, ou seja, empresas que não só tenham estabelecimento no Brasil mas que ofereçam serviços aqui no mercado brasileiro ou que colem dados pessoais no país. O prazo para adequação à nova Lei se encerra em 16 de Agosto de 2020.

Há 6 tipos de sanções administrativas como advertência com indicação de prazo para a adoção de medidas corretivas, multas simples de até 2% do faturamento no seu último exercício limitada até R\$ 50 milhões por infração ou incidente, multa diária, publicização da infração e bloqueio/eliminação dos dados pessoais a que se refere a infração.

A lei vale para todas empresas de todos os portes e de todos os setores que tratam dados pessoais



ESCOPO

O escopo da lei são dados pessoais e dados sensíveis. Dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável. O dado pessoal sensível é 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.

Capítulo 2 - Conceitos chaves



Dado Pessoal

Informação relacionada a pessoa identificada ou identificável.*

Tratamento

Qualquer operação realizada com dados pessoais.**

Titular

Pessoa a quem se referem os dados pessoais que são objeto de tratamento.

Controlador

A quem competem as decisões referentes ao tratamento de dados pessoais.***

Operador

Quem realiza o tratamento de dados pessoais em nome do controlador.**



*Os dados não são considerados como pessoais são dados anonimizados, Particulares e não econômicos, publicamente acessíveis, jornalísticos e artísticos, acadêmicos, Segurança pública, Defesa nacional, Atividade de investigação e repressão de infrações penais

** Tratamento se refere coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

*** Os agentes de tratamento, ou seja, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação a legislação de proteção de dados pessoais, é obrigado a repará-lo. O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não estiver seguindo as instruções lícitas do controlador.

Capítulo 3 - Princípios



1

Finalidade

Propósito do tratamento de dados deve ser legítimo, específico, explícito e informado ao titular.



2

Qualidade dos dados

Exatidão, clareza, relevância e atualização dos dados.



3

Livre acesso

Consulta facilitada e gratuita aos titulares sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados.



4

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular.



5

Necessidade

Limitação do tratamento de dados ao mínimo necessário.



6

Transparência

Informações claras, precisas e facilmente acessíveis sobre o tratamento de dados, observados os segredos comercial e industrial.



7

Segurança

Utilização de medidas técnicas e administrativas para evitar acessos não autorizados e situações acidentais ou ilícitas de perda, alteração, etc.



8

Prevenção

Adoção de medidas para prevenir a ocorrência de danos aos titulares.



9

Não Discriminação

Não utilização para fins discriminatórios ilícitos ou abusivos.



10

Responsabilização e Prestação de Contas

Demonstração das medidas adotadas para cumprimento das diretrizes da Lei, inclusive a eficácia destas medidas.

Capítulo 4 - Direitos dos titulares

Os titulares de dados pessoais passam a ter os seguintes direitos (Art.18):



Confirmação da existência de tratamento



Acesso aos dados



Correção dos dados incompletos, inexatos ou desatualizados



Anonimização



Portabilidade



Eliminação



Informação sobre o compartilhamento dos dados



Receber informações sobre não fornecer o consentimento e consequências



Revogação do consentimento



Titular pode peticionar contra o controlador perante a ANPD

O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. (Art.7º I)

Consentimento é toda manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (Art.5º)

O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (Art.8º § 4º)

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. (Art.8º § 5º)

Capítulo 5 - Principais Obrigações



(ART.41)

INDICAÇÃO DE ENCARREGADO(DPO)

Encarregado(DPO) é a pessoa física ou jurídica 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.37)

REGISTRO DAS OPERAÇÕES

O controlador deverá indicar encarregado pelo tratamento de dados pessoais. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.



(ART.38)

RELATÓRIO DPIA

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.



(ART.46)

SEGURANÇA DA INFORMAÇÃO

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.

Capítulo 6 - Aplicabilidade passo a passo



**INDICAÇÃO
DPO**



**MAPEAMENTO
DE DADOS**



**MEDIDAS
TÉCNICAS**



**RELATÓRIO
DPIA**

I. INDICAÇÃO DPO

- A lei prevê e exige que existam encarregados da proteção de dados pessoais DPO nas organizações.
- Recomenda-se que haja uma equipe composta por especialistas jurídicos, especialistas em segurança da informação e DPO com certificação internacional. Tal equipe poderá ser terceirizada.

II. MAPEAMENTO DE DADOS

- Elaborar e rever documentos jurídicos com a realização de eventuais adendos aos contratos existentes para a adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais.
- Exame analítico e pericial que acompanha o desempenho do tratamento dos dados na empresa, que tem por objetivo averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente e se foram implementadas com eficácia e se estão adequadas.

III. MEDIDAS TÉCNICAS

- Um processo aprofundado de estudo, análise e avaliação das informações e documentos dos diversos setores de uma empresa.
- O gerenciamento de vulnerabilidades é uma prática de segurança especificamente projetada para reduzir ou impedir de forma proativa a exploração de vulnerabilidades de TI existentes em um sistema ou organização. O processo envolve a identificação, classificação, solução e mitigação de várias vulnerabilidades em um sistema.

IV. RELATÓRIO DPIA

- Elaborar o relatório DPIA (Data Protection Impact Assessment) que 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.



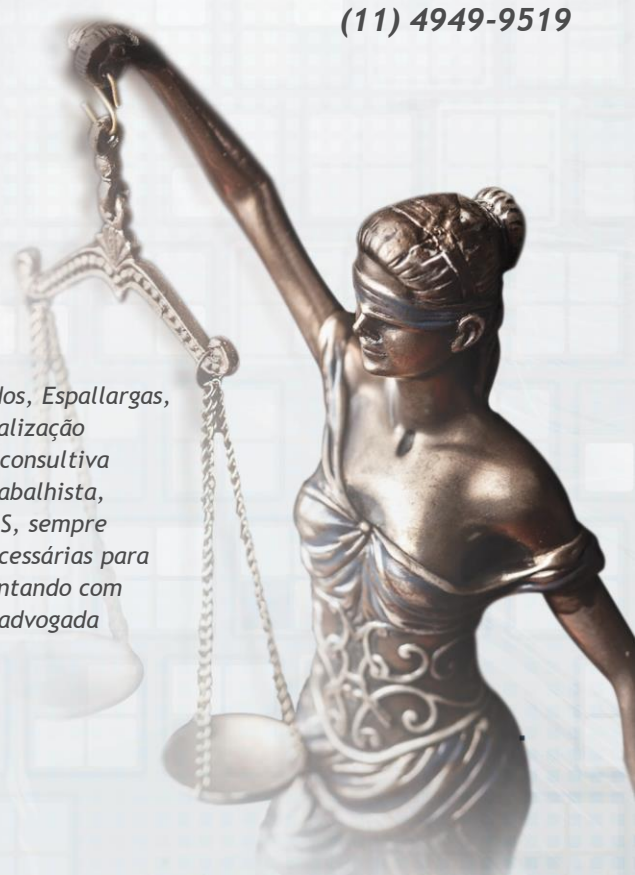


DIAZERO

SECURITY

A Diazero Security foi criada com o objetivo de suprir uma lacuna significativa na área de Segurança da Informação, seus profissionais possuem diversas graduações e prestigiadas certificações, que partem da base de governança: PMP, PSM I, ITIL, passando por Segurança Avançada sendo as certificações mais reconhecidas: ISO 27001, CEH, OSCE/OSCP, CNDA. ECSA e CCNA R&S/Security, ascendendo às novas regulamentações extraterritoriais - LGPD e GDPR, com a certificação DPO, contemplando desde uma sólida base técnica à conformidade com a legislação na companhia de nossos associados.

OSCAR ANTONANGELO
oscar@diazerosecurity.com.br
(11) 4949-9519



Espallargas . Gonzalez . Sampaio

ADVOGADOS

Fundado em 1988 e resultado da reunião de experientes advogados, Espallargas, Gonzalez & Sampaio - Advogados têm ênfase na permanente atualização e modernização da prestação de serviços jurídicos, com atuação consultiva e contenciosa nas áreas do Direito Administrativo, societário, Trabalhista, Tributário e Cível. Após a promulgação da Lei 13709/2018, a EGS, sempre inovando, buscou soluções para implementação das medidas necessárias para dirimir os possíveis riscos de seus clientes no tocante à LGPD, contando com a dedicação para este tema da Dra. Claudia Fabiana Giacomazi, advogada graduada pela Pontifícia Universidade Católica - PUC - SP.

CLAUDIA GIACOMAZI
claudia.giacomazi@egsadvogados.com.br
(11) 3371-2890

