



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



LGPDF™ Versão 092021

CertiProf®

Exame LGPD Fondation (LGPFD)

IV - Público-alvo

Esta certificação destina-se a profissionais advindos das áreas de: Direito Digital, Tecnologia da Informação, Segurança da Informação, Governança, Risco e Compliance, além de áreas impactadas pela Lei Geral de Proteção de Dados. Esta certificação também destinasse a aqueles que desejam conhecer a fundo a lei e seu impacto nas instituições, nos usuários e na sociedade.

V - Carga Horária

A recomendação é que a carga horária do treinamento de certificação seja de 8 horas em classe e 8 horas de auto estudo através das referências bibliográficas recomendadas. Durante o treinamento podem ser aplicadas dinâmicas de estudo, preparação para o exame e exercícios para a melhor compreensão e memorização do conteúdo.

Tipo de Prova	Múltipla Escolha
Questões	40
Pontuação Necessária	80%
Tempo do exame	60 minutos

Quem é CertiProf®?

CertiProf® é um instituto de exames fundado nos Estados Unidos em 2015. Localizado em Sunrise, Flórida.

Nossa filosofia é baseada na criação de conhecimento na comunidade e para isso, sua rede colaborativa é composta por:

- **CKA (Embaixadores do Conhecimento CertiProf)**, são influenciadores em suas áreas de especialização ou especialização, treinadores, consultores, blogueiros, construtores de comunidades, organizadores e evangelistas, que estão dispostos a contribuir para melhorar o conteúdo
- **Os CLL (CertiProf Lifelong Learners)** são identificados como alunos contínuos que demonstraram seu compromisso inabalável com a aprendizagem ao longo da vida, que é de vital importância no mundo digitalizado em constante mudança e expansão de hoje. Independentemente de ganharem ou não o exame
- **ATP's (Parceiros Formadores Credenciados)**, Universidades, centros de formação e facilitadores de todo o mundo que integram a rede de parceiros
- **Autores (co-criadores)**, Especialistas ou profissionais da indústria que, com seu conhecimento, desenvolvem conteúdo para a criação de novas certificações que atendam às necessidades da indústria
- **Equipe interna**, nossa equipe distribuída com operações na Índia, Brasil, Colômbia e Estados Unidos que apóiam dia a dia a execução do propósito da **CertiProf®**

Our Accreditations and Affiliations



Lifelong Learning

Os ganhadores deste distintivo específico provaram seu compromisso inabalável com a aprendizagem ao longo da vida, que é de vital importância no mundo digitalizado em constante mudança e expansão de hoje. Também identifica as qualidades de uma mente aberta, disciplinada e em constante evolução, capaz de usar e contribuir com seus conhecimentos para o desenvolvimento de um mundo mais igual e melhor.

Critérios de ganho:

- Seja um candidato à certificação CertiProf®
- Seja um aluno contínuo e focado
- Identifique-se como conceito de aprendizagem ao longo da vida
- Acredite verdadeiramente e se identifique com o conceito de que o conhecimento e a educação podem e devem mudar o mundo
- Quer impulsionar seu crescimento profissional



COMPARTILHE E VERIFIQUE

AS SUAS REALIZAÇÕES DE
APRENDIZAGEM COM FACILIDADE

#LGPDF #CertiProf



AGENDA

Módulo 1: Contextualização	8
O que é privacidade de dados?	9
O que acontece em 1 minuto de internet?	9
Dados Pessoais São Uma Moeda de Troca	10
Por que a privacidade importa para todos?	10
Exposição de Dados Sensíveis é um dos Principais Riscos	11
Privacidade de Dados não é a Mesma Coisa que Segurança de Dados	11
O que as Empresas Precisam Aprender?	12
Consequências de não Conformidade	12
Existem Cada vez Mais Regulamentos de Privacidade em Todo o Mundo	13
Multas - GDPR e LGPD	13
Multas Aplicadas com Base no GDPR	14
Onde Consultar Multas Aplicadas com Base no GDPR?	14
Onde Consultar Multas Aplicadas com Base na LGPD?	15
A Lei Geral de Proteção de Dados Pessoais (LGPD) Lei Federal n.º 13.709/2018	15
Onde acessar a LGPD?	15
Módulo 2: Introdução à LGPD e Fundamentos	16
Estrutura da LGPD	17
Propósito da LGPD	18
Termos-chave da LGPD	18
Fundamentos	18
Escopo Territorial	19
Quando a LGPD não se aplica?	19
Termos-chave da LGPD	20
Princípios	22
Princípios e a Demonstração de Adequação à LGPD	23
Princípios	23
Módulo 3: Bases Legais Para o Tratamento de Dados Pessoais	24
Em qual parte da lei estamos?	25
Seção I	25
Bases Legais na LGPD	25
Hipóteses Para o Tratamento de Dados Pessoais	26
Consentimento	27
Interesse Legítimo	27
Seção II	27
Hipóteses Para o Tratamento de Dados Pessoais Sensíveis	28
Dados Anonimizados	28
Acesso por Órgãos de Pesquisa	28
Seção III	29
Tratamento de Dados Pessoais de Crianças e de Adolescentes	29
Seção IV	29
Quando ocorre o término do tratamento?	29
Eliminação dos Dados Pessoais	30

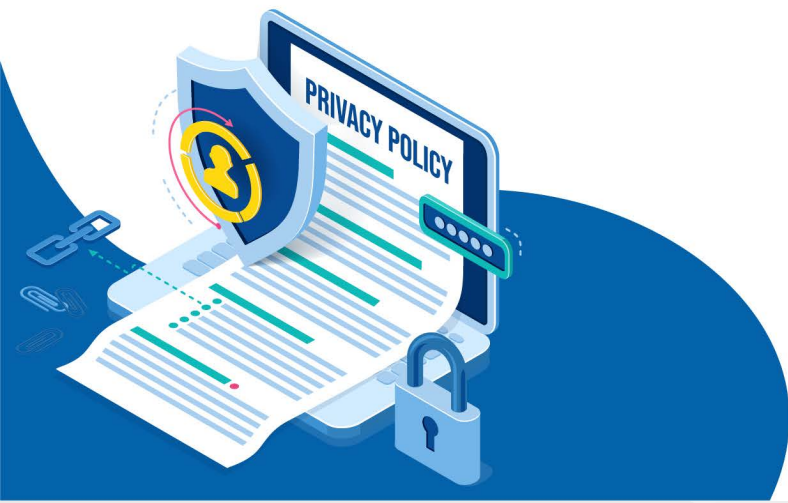
Módulo 4: Direitos do Titular - Teórica & Prática	31
Em qual parte da lei estamos?	32
Direitos do Titular	32
Resumo dos Direitos do Titular	34
Direitos do Titular	34
Módulo 5: Tratamento de Dados Pessoais Pelo Poder Público	38
Em qual parte da lei estamos?	39
Premissas	39
Seção I	40
Quando é permitido o tratamento de dados pessoais?	40
No Caso de Empresas Públicas e as Sociedades de Economia Mista	41
Formato Interoperável Para Uso Compartilhado	42
Uso Compartilhado de Dados Pessoais	42
Uso Compartilhado de Dados Pessoais com Consentimento do Titular	42
Registros das Operações de Tratamento	43
Publicação RIPD e Ações de Padrões e Boas Práticas	43
Registros das Operações de Tratamento	43
Seção II	43
Em Caso de Violação	43
Módulo 6: Transferência Internacional de Dados	44
Em qual parte da lei estamos?	45
Quando a transferência internacional é permitida?	45
Nível de Proteção Exigido do País Estrangeiro	46
Garantias Mínimas	46
Módulo 7: Agentes de Tratamento de Dados Pessoais	47
Em qual parte da lei estamos?	48
Lembrando	48
Seção I	48
Registro de Tratamento de Dados	49
Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	50
Operador x Controlador	52
Outras Obrigações dos Agentes de Tratamento	52
Padrões de Interoperabilidade	52
Seção II	52
Seção III	52
Reparação de Danos	53
Quando agentes não serão responsabilizados?	53
Quando o tratamento é considerado irregular?	53
Violação do Direito do Titular	53
Módulo 8: Encarregado (ou DPO)	54
Em qual parte da lei estamos?	55
Lembrando	55
Dica Prática!	56
Nomeação de um Encarregado	56

Quem pode ser um encarregado?	57
Atividades de um Encarregado	57
Um DPO Pode Atender a Várias Organizações	58
Qualificações Recomendadas	58
Qualificações Recomendadas Para um DPO	58
Onde estão os DPOs no mundo?	59
Perfil do DPO no Brasil (ANPPD, 2020)	59
17 Conhecimentos Específicos para um DPO/Encarregado	60
Alguns Regulamentos que um DPO no Brasil Precisa Conhecer	61
Módulo 9: Segurança e Boas Práticas - Teórica & Prática	62
Em qual parte da lei estamos?	63
Seção I	63
Adoção de Medidas	63
Comunicação do Incidente de Segurança	64
Seção II	65
Boas Práticas e da Governança	65
Objetivos de Controles da ISO 27001	66
Cyber-ataques em Tempo Real	66
Já tive dados pessoais vazados?	67
Onde buscar ferramentas para LGPD?	68
Por onde começar a Política de Segurança?	69
Módulo 10: Sanções Administrativas	70
Em qual parte da lei estamos?	71
Responsabilização	71
Aplicação de Sanções Administrativas	71
Sanções Previstas	72
Critérios para Aplicação Das Sanções	72
Fiscalização por Outros Órgãos	73
Destino das Arrecadações	73
Módulo 11: Autoridade Nacional de Proteção de Dados (ANPD)	74
Em qual parte da lei estamos?	75
Autoridade Nacional de Proteção de Dados - ANPD	75
Criação da ANPD	76
Composição da ANPD	76
Problemática	76
Atribuições da ANPD	76
Competências da ANPD	77
Cooperação da ANPD com Outros Órgãos	77
Relacionamento ANPD	78
Conselho Nacional de Proteção de Dados (CNPd)	78
Fiscalização por Outros Órgãos	79
Destino das Arrecadações	79
Referências	80

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



Módulo 1: Contextualização



LGPDF™ Versão 092021

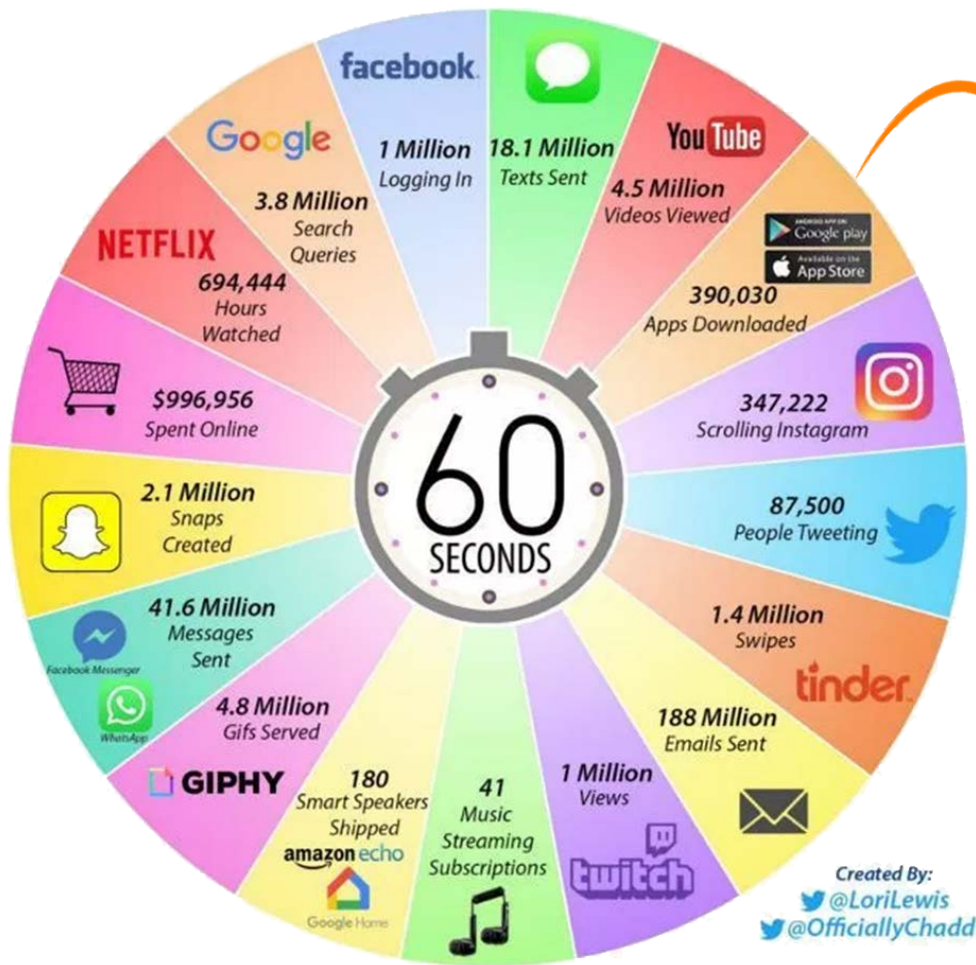
CertiProf®

O que é privacidade de dados?

- É a **habilidade de uma pessoa** em controlar a exposição e a disponibilidade de informações acerca de si (Dicionario Informal)
- Condição daquilo que é **privado, pessoal, íntimo** (Dicionário Priberam)
- É o direito **ao respeito pela vida privada de uma pessoa**, em seu âmbito familiar e de sua correspondência
- Dependerá de **como os dados são coletados, armazenados e compartilhados** com terceiros, além da conformidade com as leis de privacidade aplicáveis



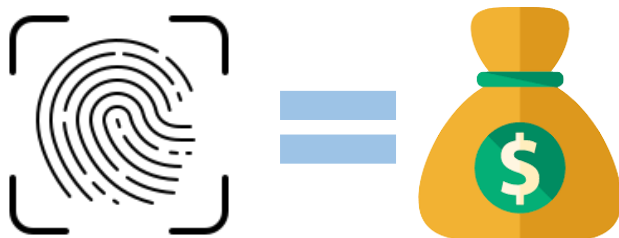
O que acontece em 1 minuto de internet?



Os dados
são de
2019

Dados Pessoais São Uma Moeda de Troca

“Quando você não paga por algo no mundo digital, a mercadoria é você.”



O aplicativo FaceApp se tornou uma grande sensação quando foi lançado, levando milhões de pessoas por todo o mundo a usarem a tecnologia de reconhecimento facial para mostrarem aos seus amigos como seriam se fossem mais velhos ou mais novos. Entretanto, houve muitas suspeitas de roubos de dados via esse app.



Por que a privacidade importa para todos?

1. **Limite de poder:** Quanto mais alguém sabe sobre nós, mais poder pode ter sobre nós. É adequado limitar o poder que as empresas podem ter sobre nós
2. **Respeito pelas pessoas:** Privacidade é respeitar pessoas. Se uma pessoa tem um desejo de manter algo em sigilo, é desrespeitoso ignorar os seus desejos sem uma razão convincente
3. **Gestão da reputação:** A privacidade permite que possamos gerenciar nossa reputação. O modo como somos julgados pelos outros afeta nossas oportunidades, amizades e bem-estar geral
4. **Manutenção de limitações sociais:** As pessoas estabelecem limites dos outros na sociedade. Esses limites são físicos e informativos. Por exemplo, ninguém precisa saber onde estamos em todos os momentos
5. **Confiança:** Nos relacionamentos, sejam pessoais, profissionais, governamentais ou comerciais, dependemos de confiar na outra parte. Violações de confidencialidade são violações dessa confiança. Você confiaria em uma empresa que promete usar seus dados para uma finalidade e usa para outra?
6. **Controle sobre a nossa vida:** Sem termos conhecimento de quais dados estão sendo usados, como estão sendo usados, a capacidade de corrigi-los e alterá-los, estamos praticamente desamparados no mundo de hoje
7. **Liberdade de pensamento e fala:** Privacidade é a chave para a liberdade de pensamento. Um olhar atento sobre tudo o que lemos ou assistimos pode nos impedir de explorar outros pensamentos
8. **Liberdade de atividades políticas e sociais:** A privacidade ajuda a proteger nossa capacidade de nos associarmos a outras pessoas e participar de atividades políticas
9. **Não ter que se explicar ou se justificar:** Pode ser pesado demais se tivermos que pensar em como tudo o que fazemos será percebido pelos outros e que teremos que estar prontos para explicar situações embaraçosas
10. **Capacidade de mudar e ter segundas chances:** As pessoas estão em constante evolução; nós mudamos e crescemos ao longo da vida. Existe um grande valor na capacidade de ter uma segunda chance, ser capaz de aprender com o erro, ser capaz de se reinventar. É justo uma pessoa ser julgada eternamente por algum comentário postado em uma rede social?

Exposição de Dados Sensíveis é um dos Principais Riscos



- A OWASP é uma organização sem fins lucrativos e foi fundada nos EUA em 2004
- Ela realizou um levantamento global e colaborativo com os 10 riscos de segurança mais críticos da web, conhecido como OWASP TOP 10

- A1 Injeção de código
- A2 Quebra de autenticação
- A3 Exposição de dados sensíveis
- A4 Entidades Externas XML
- A5 Quebra de controle de acesso
- A6 Má configuração de segurança
- A7 Cross-site Scripting (XSS)
- A8 Desserialização insegura
- A9 Usar componentes com vulnerabilidades conhecidas
- A10 Registro e monitoração ineficientes

Privacidade de Dados não é a Mesma Coisa que Segurança de Dados

Segurança de dados



Privacidade de dados

A **segurança de dados** diz respeito aos **meios de proteção** que uma organização está adotando **para impedir que terceiros não autorizados acessem** os seus dados.

Ela se concentra na proteção de dados contra ataques maliciosos e impede a exploração de dados (violação de dados ou ciberataque).

Inclui controles de acesso, criptografia, segurança de rede, etc.

A **privacidade de dados** se concentra nos **direitos dos indivíduos**, na finalidade de coleta e processamento de dados, nas preferências de privacidade e na maneira como as organizações controlam os dados pessoais dos titulares de dados.

Ela se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados de acordo com a lei.

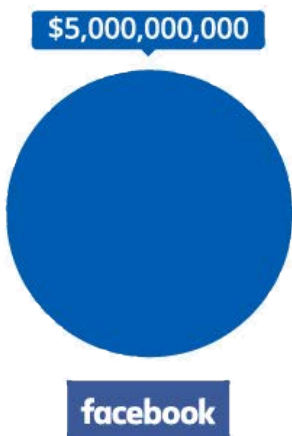
O que as Empresas Precisam Aprender?

- Na era da economia de dados, o verdadeiro **valor da empresa está nos dados coletados do cliente**
 - Isso significa que os dados são um ativo digno de proteção e manutenção
- Os **dados pessoais** dos indivíduos processados pelas empresas **são apenas emprestados**, não são de propriedade das empresas
- **Para que as empresas mantenham os dados e sigam a confiança, elas terão que demonstrar transparência** ao se comunicar abertamente sobre quais dados coletam, para quais finalidades, quem é o seu **processador de dados** e assim por diante



Consequências de não Conformidade

- É muito arriscado para as empresas não estarem em conformidade com as leis de privacidade
- As empresas correm o risco de multas e ações judiciais, sem mencionar a **perda da reputação e da fidelidade do cliente**



Multa estabelecida pelo Departamento de Proteção ao Consumidor dos EUA por não ter atendido a um pedido de proteção de privacidade dos clientes em 2012.



Violação de dados afetando 147 milhões de clientes em 2017.



Violação de dados afetando 500.000 clientes em 2018.



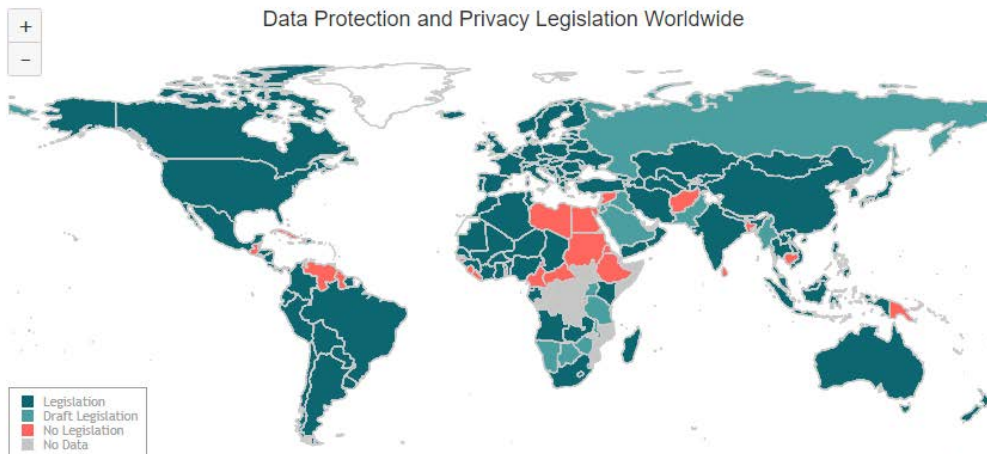
Violação de dados afetando 57 milhões de clientes em 2016.

Algumas das maiores multas já aplicadas até hoje

Existem Cada vez Mais Regulamentos de Privacidade em Todo o Mundo

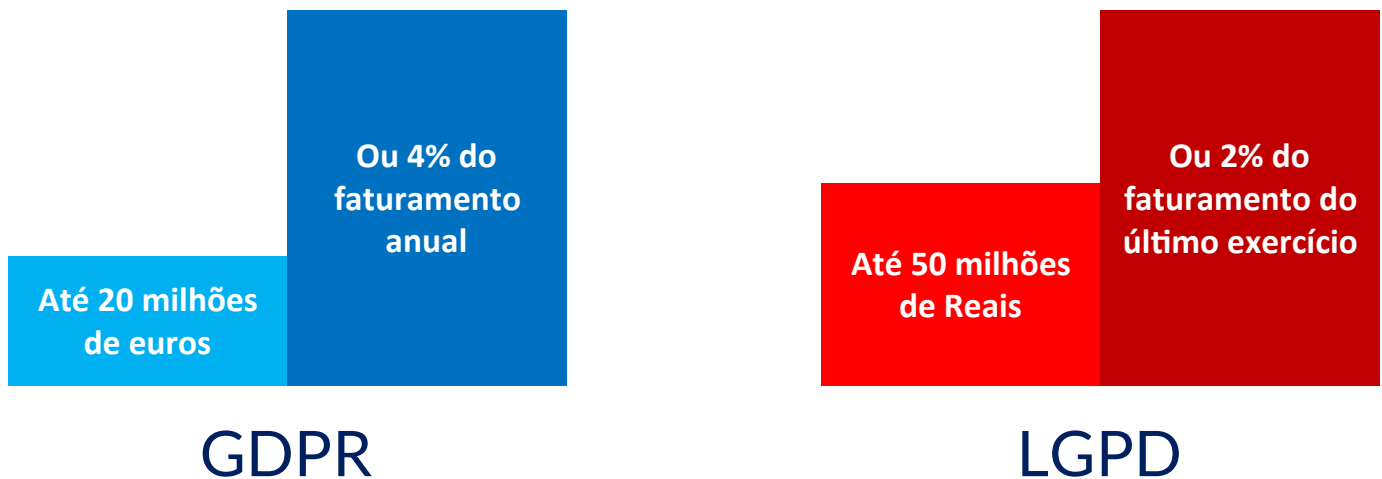


Países: Regiões: Baixar:



Fonte: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Multas - GDPR e LGPD



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS LGPDF™

Multas Aplicadas com Base no GDPR

237 multas
€ 467.569.168

➤ **Maior:** € 204,600,000
➤ **Menor:** € 118,00

Motivo das multas :

- 1) Falhas em Base Jurídica (104)
- 2) Falhas em Segurança da Informação (63)

Países com multas mais altas:

- 1) Reino Unido
- 2) França
- 3) Itália

Países que mais multaram:

- 1) Espanha (80)
- 2) Romênia (27)
- 3) Alemanha (25)

Segmentos multados:

- 1) Aviação
- 2) Hotéis
- 3) Serviços
- 4) Operadoras
- 5) Buscadores
- 6) Org. Públicos

Fonte: GDPR Enforcement Tracker

ANPPD
Associação Nacional dos Profissionais de Privacidade de Dados

Onde Consultar Multas Aplicadas com Base no GDPR?

Norway: Possible new fine on Bergen Municipality
Datatilsynet intends to impose a fine of EUR 275.000 on the Bergen Municipality for inadequate data security: link

GDPR Enforcement Tracker tracked by **C/M'S** Law.Tax

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties.

Show 10 entries

Country	Authority	Date	Fine [C]	Controller/Processor	Quoted Art.	Type	Infos
UNITED KINGDOM	Information Commissioner (ICO)	2019-07-08	204,600,000	British Airways	Art. 32 GDPR	Insufficient technical and organisational measures	link

Fonte: <https://www.enforcementtracker.com/>

Onde Consultar Multas Aplicadas com Base na LGPD?

PORTAL DAS VIOLAÇÕES - LGPD

O "Violações LGPD" é um serviço de consulta pública gratuita que reúne as atuações relacionadas com privacidade de dados (sob a ótica da LGPD - Lei Geral de Proteção de Dados, e outras normas relacionadas ao tema) impostas por diversos órgãos brasileiros uma vez já tornadas públicas e publicadas nos sites das autoridades. Nem todas as tramitações tornam-se públicas, portanto podem existir atuações não listadas.

Data	Estado	Sanções	Emissor	Status	Penalidade	Valor [R\$]	Condenações	Segmento	Lei
15/07/2021	SP	Judiciais	TJ/SP	1ª Instância	Outras	R\$ 5.000,00	Indenização por Danos Morais	Transporte	LGF

Fonte: <https://anppd.org/violacoes>

A Lei Geral de Proteção de Dados Pessoais (LGPD) Lei Federal n.º 13.709/2018

Regulamenta

o uso, a proteção e a transferência de dados pessoais de pessoas naturais (pessoas físicas).

Violações

podem levar desde a suspensão das atividades de coleta de dados pessoais a multas de até R\$ 50 milhões.

Aprovada em 2018

LGPD

Lei Geral de Proteção de Dados

Inspirada no GDPR.

Obriga todas as empresas a investir em cibersegurança

e implementar sistemas de compliance efetivos a fim de prevenir, identificar e mitigar violações de dados pessoais dos clientes.

Exige nomeação de um Encarregado.

Onde acessar a LGPD?



Disponível online

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

www.certiprof.com



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



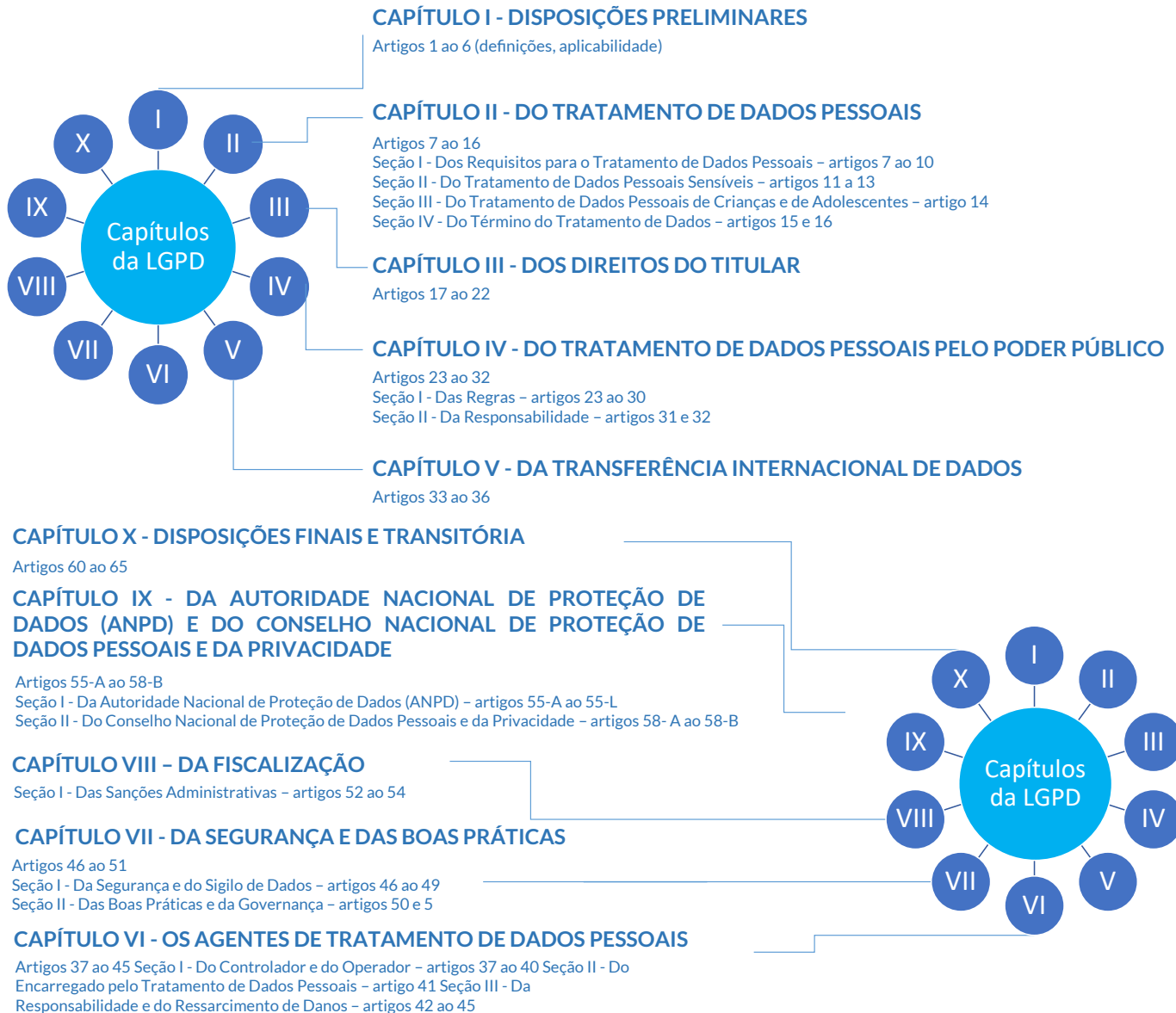
Módulo 2: Introdução à LGPD e Fundamentos



LGPDF™ Versão 092021

CertiProf®

Estrutura da LGPD



Propósito da LGPD

- **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**.
 - **Parágrafo único.** As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios



Termos-chave da LGPD



Fundamentos

Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos:

1. O respeito à privacidade
2. A autodeterminação informativa
3. A liberdade de expressão, de informação, de comunicação e de opinião
4. A inviolabilidade da intimidade, da honra e da imagem
5. O desenvolvimento econômico e tecnológico e a inovação
6. A livre iniciativa, a livre concorrência e a defesa do consumidor
7. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais

Escopo Territorial

Art. 3º. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional



II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional



III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.



Art. 3º, III

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Quando a LGPD não se aplica?

Art. 4º. Esta Lei não se aplica ao tratamento de dados pessoais:

1. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos
 - O artigo 3.o, n.o 2, segundo travessão, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que a exploração de um sistema de câmera que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição

(Fonte: Tribunal de Justiça (Quarta Secção) de 11 de dezembro de 2014, Processo C-212/13. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62013CJ0212>)

2. Realizado para fins exclusivamente:
 - a) Jornalístico e artísticos
 - b) Acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei
3. Realizado para fins exclusivos de:
 - a) Segurança pública
 - b) Defesa nacional
 - c) Segurança do Estado
 - d) Atividades de investigação e repressão de infrações penais

4. 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

Termos-chave da LGPD

Art. 5º. Para os fins desta Lei, considera-se:

- I. **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável
- II. **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
- IV. **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Dado pessoal:

Para fins do Decreto nº 10.046/2019 (Cadastro Base do Cidadão e o Comitê Central de Governança de Dados), considera-se:

- 1. **Atributos biográficos** - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios
- 2. **Atributos biométricos** - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar
- 3. **Dados cadastrais** - informações identificadoras perante os cadastros de órgãos públicos, tais como:
 - a) O número de inscrição no Cadastro de Pessoas Físicas – CPF
 - b) O número de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ
 - c) Outros dados públicos relativos à pessoa jurídica ou à empresa individual
- 4. **Atributos genéticos** - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas (...)

Art. 5º. Para os fins desta Lei, considera-se:

- III. **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
- XI. **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 (+ art. 12)
- V. **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
- VI. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
- VII. **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
- IX. **Agentes de tratamento:** o controlador e o operador
- VIII. **Encarregado:** 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)

Obs: Art. 41, par. 4: foi retirada a necessidade de conhecimento jurídico-técnico do encarregado de proteção de dados pessoais, porém, na prática, identifica-se a obrigatoriedade.

Information (name)	Anonymized
Peter	*****
Annabelle	*****
Mark	*****
Elizabeth	*****
Mark	*****
Annabelle	*****



São dados pessoais convertidos em dados não identificáveis, cujo processo de anonimização não pode ser reversível.

- XI. Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda como tratamento de seus dados pessoais para uma finalidade determinada
- XII. Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados
- XIII. Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
- XIV. Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
- XV. Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados
- XVI. 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
- XVIII. Órgão de pesquisa:** órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
- XIX. Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

Princípios

Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:



Para Miguel Reale, o legislador, quando da redação da lei, reconhece que o "sistema de leis não é suscetível de cobrir todo o campo da experiência humana, restando sempre grande número de situações imprevistas, algo que era impossível ser vislumbrado."

Para essas lacunas do direito, "há a possibilidade do recurso aos princípios gerais de direito, mas é necessário advertir que a estes não cabe apenas essa tarefa de preencher ou suprir as lacunas da legislação" (1998, p. 306).

(REALE, Miguel. *Lições Preliminares de Direito*. 24. ed. São Paulo: Saraiva, 1998.

CUNHA, Guilherme Bohrer Lopes. *A situação atual da teoria dos princípios no Brasil*. *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 15, n. 2410, 5 fev. 2010. Disponível em: <https://jus.com.br/artigos/14289>. Acesso em: 12 jun. 2020).

Violar um princípio é muito mais grave que transgredir uma norma qualquer. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou de inconstitucionalidade, conforme o escalão do princípio atingido, porque representa insurgência contra todo o sistema, subversão de seus valores fundamentais, contumélia irremissível a seu arcabouço lógico e corrosão de sua estrutura mestra. Isto porque, com ofendê-lo, abatem-se as vigas que os sustentam e alui-se toda a estrutura nelas esforçada."

(MELLO, Celso Antônio Bandeira de, *Curso de Direito Administrativo*. 12ª ed. - São Paulo : Malheiros, 2000, p. 747/748.)

Princípios e a Demonstração de Adequação à LGPD

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos:

- Requisitos de segurança
- Aos padrões de boas práticas e de governança e
- Aos princípios gerais previstos nesta Lei e às demais normas regulamentares

Princípios

1. **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
2. **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento
3. **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados
4. **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais
5. **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
6. **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial
7. **Segurança:** utilização de medidas 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 difusão
8. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
9. **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
10. **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



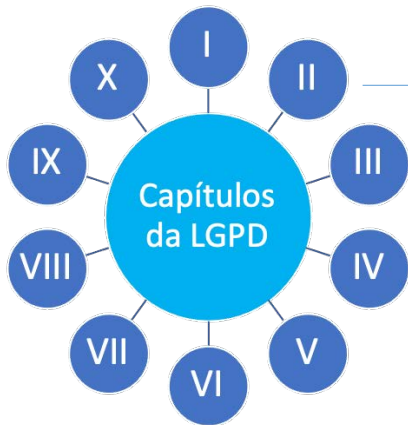
Módulo 3: Bases Legais Para o Tratamento de Dados Pessoais



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO II - DO TRATAMENTO DE DADOS PESSOAIS

Artigos 7 ao 16

Seção I - Dos Requisitos para o Tratamento de Dados Pessoais – artigos 7 ao 10

Seção II - Do Tratamento de Dados Pessoais Sensíveis – artigos 11 a 13

Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes – artigo 14

Seção IV - Do Término do Tratamento de Dados – artigos 15 e 16

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Bases Legais na LGPD



Hipóteses Para o Tratamento de Dados Pessoais

Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

1. Mediante o fornecimento de **consentimento** pelo titular
2. Para o cumprimento de **obrigação legal ou regulatória** pelo controlador
3. **Pela administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei
4. Para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais
5. 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**
6. 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)
7. Para a **proteção da vida** ou da incolumidade física do titular ou de terceiro
8. Para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
9. Quando necessário para atender aos **interesses legítimos** do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais
10. Para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente

Art. 7º :

- § 1º. (revogado)
- § 2º. (revogado)
- § 3º. O tratamento de dados pessoais cujo **acesso é público** deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização
- § 4º. É dispensada a exigência do consentimento previsto no caput deste artigo para os dados **tornados manifestamente públicos** pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei
- § 5º. O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei
- § 6º. A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular
- § 7º. O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei

Consentimento

Art. 8º. O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

- § 1º. Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais
- § 2º. Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei
- § 3º. É vedado o tratamento de dados pessoais mediante vício de consentimento
- § 4º. O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas
- § 5º. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei
- § 6º. Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração

Interesse Legítimo

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:

1. Apoio e promoção de atividades do controlador
 2. 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
- § 1º. Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados
 - § 2º. O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse
 - § 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

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Hipóteses Para o Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

1. Quando o titular ou seu responsável legal consentir, de forma **específica e destacada**, para finalidades específicas
2. 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 terceiro
 - f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
 - 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 prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

Dados Anonimizados

Art. 12. Os dados anonimizados **não serão considerados dados pessoais** para os fins desta Lei, **salvo quando o processo de anonimização ao qual foram submetidos for revertido**, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

- § 1º. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios
- § 2º. Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada
- § 3º. A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais

Acesso por Órgãos de Pesquisa

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Seção III

Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

- § 1º. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal
- § 2º. No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei
- § 3º. Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo
- § 4º. Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade
- § 5º. O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis
- § 6º. As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança

Seção IV

Do Término do Tratamento de Dados

Quando ocorre o término do tratamento?

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

1. Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada
2. Fim do período de tratamento
3. Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público
4. Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei

Eliminação dos Dados Pessoais

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

1. Cumprimento de obrigação legal ou regulatória pelo controlador
2. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
3. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei
4. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



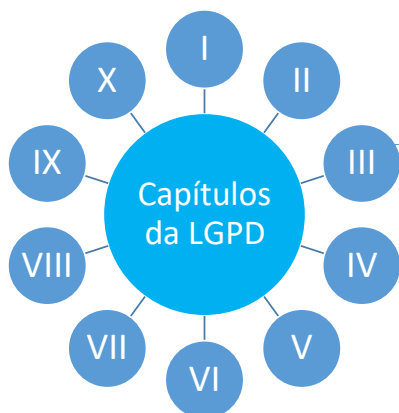
Módulo 4: Direitos do Titular - Teórica & Prática



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO III - DOS DIREITOS DO TITULAR

Artigos 17 ao 22

Direitos do Titular

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

1. Confirmação da existência de tratamento
 2. Acesso aos dados
 3. Correção de dados incompletos, inexatos ou desatualizados
 4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei
 5. 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
 6. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei
 7. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
 8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
 9. Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei
- § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional
 - § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei
 - § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento

- § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
 1. Comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente
 2. Indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
- § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento
- § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional
- § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador
- § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

1. Em formato simplificado, imediatamente
 2. Por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular
- § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
 - § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
 - I. Por meio eletrônico, seguro e idôneo para esse fim
 - II. Sob forma impressa

Art. 20. O titular dos dados tem direito a solicitar a **revisão de decisões** tomadas unicamente com base em **tratamento automatizado** de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

- § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial
- § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Resumo dos Direitos do Titular



Direitos do Titular

PARTE PRÁTICA: DPO e os Direitos dos Titulares

Conformidade da LGPD nos Portais WEB:

- Divulgação do DPO (Art. 41)
- Princípio da Minimização (Art. 6, III - LGPD)
- Direito de Acesso e Correção (Artigo 18, II, III - LGPD)
- Direito de Eliminação dos Dados (Artigo 18, V LGPD)
- Registro das Operações de Tratamento (Artigo 37 - LGPD)
- Direito de Portabilidade (Artigo 18, V - LGPD)

Estudo de Caso Público: ANPPD.org

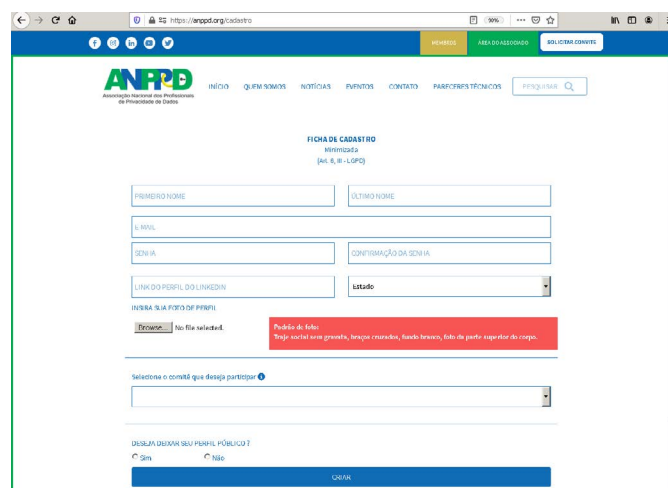
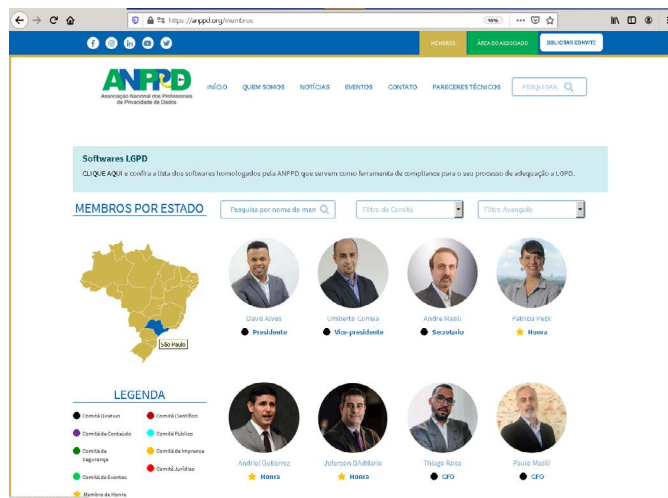


Estudo de Caso Público: ANPPD.org

O Portal da ANPPD foi um dos primeiros websites do Brasil a oferecer os Direitos dos Titulares. Na imagem ao lado vemos a FINALIDADE primária de exposição dos profissionais no mapa de membros.

Para que a finalidade seja atingida, o profissional deve preencher uma FICHA DE CADASTRO que esta minimizada e referenciada com o Art. 6, III. Essa é a porta de entrada dos dados pessoais pelo controlador. Importante notar que ainda na página existe um link para a Política de Privacidade da instituição.

A Política de Privacidade pode ser visualizada na “Área LGPD” contida em “Quem Somos”. Como exemplo, é importante que os controladores ofereçam fácil acesso em caso dos titulares desejarem obter mais informações sobre o tratamento dos dados pessoais.



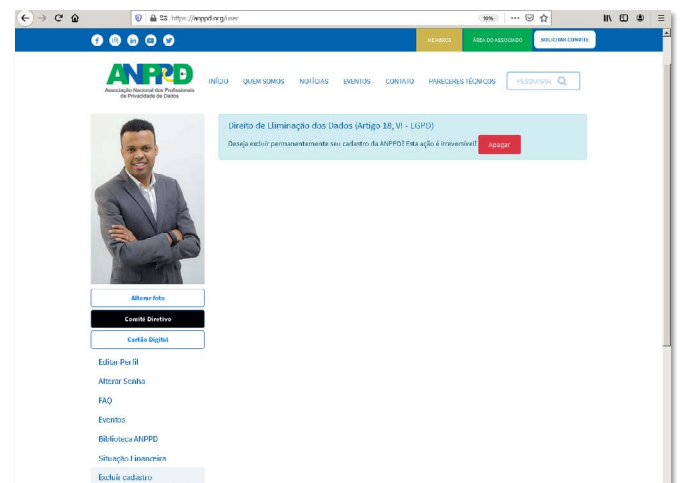
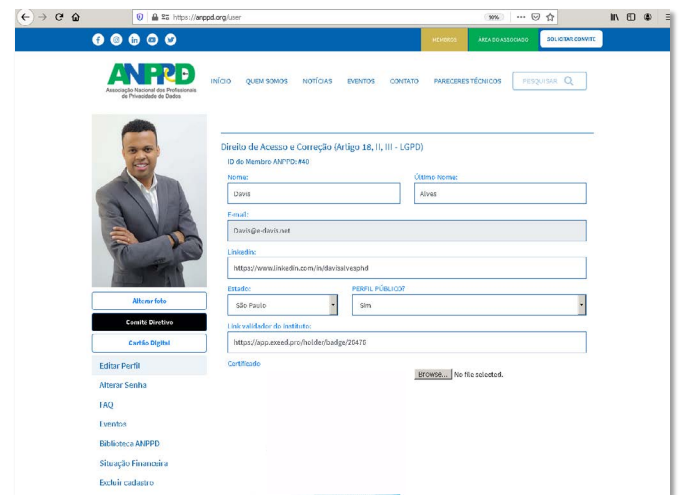
Também junto à Política de Privacidade é recomendável publicar as informações sobre o Encarregado pelo Tratamento de Dados Pessoais (art. 41) responsável, juntamente com sua equipe de trabalho.

Uma vez enunciado na Política de Privacidade, os titulares podem ver seu cumprimento seguindo as instruções informadas.

Como exemplo, na imagem ao lado é apresentado o **Direito de Acesso e Correção** dos dados inseridos no momento do cadastro, em conformidade com o Art. 18, II e III - LGPD).

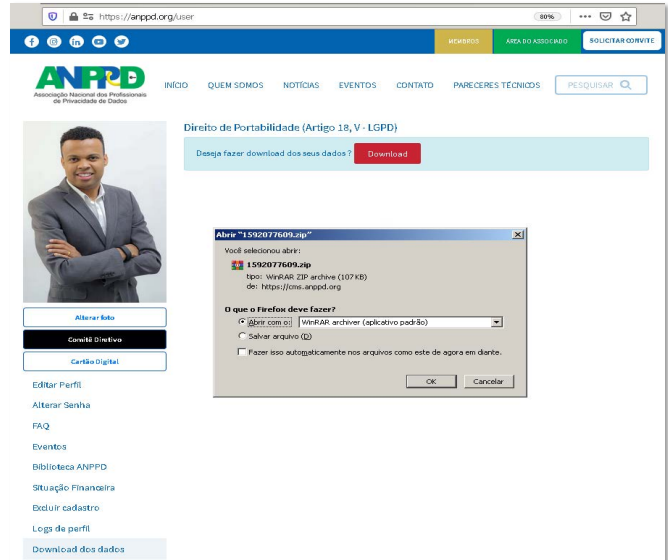
Uma vez enunciado na Política de Privacidade, os titulares podem ver seu cumprimento seguindo as instruções informadas.

Como exemplo, na imagem ao lado é apresentado o **Direito de Eliminação** dos dados inseridos no momento do cadastro, em conformidade com o Art. 18, VI - LGPD).



Uma vez enunciado na Política de Privacidade, os titulares podem ver seu cumprimento seguindo as instruções informadas.

Como exemplo, na imagem ao lado é apresentado o Direito da Portabilidade inseridos no momento do cadastro, em conformidade com o Art. 18, V – LGPD).



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



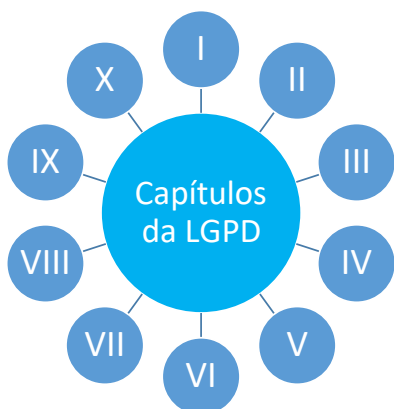
Módulo 5: Tratamento de Dados Pessoais Pelo Poder Público



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Artigos 23 ao 32
Seção I - Das Regras - artigos 23 ao 30
Seção II - Da Responsabilidade - artigos 31 e 32

Premissas

- Constituição da República Federativa do Brasil de 1988. Acesso em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
- **Administração Pública** = conjunto de órgãos, serviços e agentes do Estado que procura satisfazer as necessidades da sociedade, tais como: educação, cultura, segurança, saúde
- **Administração Pública** é a gestão dos interesses públicos por meio da prestação de serviços públicos

(Fonte: Gregorius, Marcio Rosni. 2015. <https://marciorosni.jusbrasil.com.br/artigos/195654350/a-administracao-publica-e-suas-funcoes>).

Constituição Federal

Art. 3º. Constituem objetivos fundamentais da República Federativa do Brasil:

1. Construir uma sociedade livre, justa e solidária
2. Garantir o desenvolvimento nacional
3. Erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais
4. Promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação

Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios **obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:**

- § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:
 - II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; (Incluído pela Emenda Constitucional nº 19, de 1998)

Art. 5:

- X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação
- XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamento) (Vide Lei nº 12.527, de 2011)

Seção I

Das Regras

Quando é permitido o tratamento de dados pessoais?

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei de Acesso à Informação, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

Pessoas jurídicas de direito público:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

1. Os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público
2. As autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios

Informações sobre o tratamento no site

1. Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos
2. II e IV – VETADOS (proibição de compartilhamento de dados, bem como com pessoas jurídicas de direito privado) – ago/2018

“Ouvido, o Ministério da Fazenda manifestou-se pelo veto ao seguinte dispositivo: Inciso II do art. 23

‘II - sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), **vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado.**’

Razões do veto: ‘O dispositivo veda o compartilhamento de dados pessoas no âmbito do Poder Público e com pessoas jurídicas de direito privado. Ocorre que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. É o caso, por exemplo, do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, cujas informações são utilizadas para o reconhecimento do direito de seus beneficiários e alimentados a partir do compartilhamento de diversas bases de dados administrados por outros órgãos públicos. Ademais, algumas atividades afetas ao poder de polícia administrativa poderiam ser inviabilizadas, a exemplo de investigações no âmbito do Sistema Financeiro Nacional, dentre outras.’”

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei de Acesso à Informação, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

Quando essas pessoas jurídicas forem operadoras, deverão indicar um encarregado

- III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei

No Caso de Empresas Públicas e as Sociedades de Economia Mista

Se explorarem atividade econômica, podem ter o mesmo tratamento das PJs de direito privado

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

- Parágrafo único. **As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo**

Formato Interoperável Para Uso Compartilhado

Art. 25. Os dados deverão ser mantidos em **formato interoperável** e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.



Uso Compartilhado de Dados Pessoais

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

- § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
 1. Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação
 2. (VETADO)
 3. Nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei
 4. Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres
 5. Na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades

Uso Compartilhado de Dados Pessoais com Consentimento do Titular

Regra: compartilhamento de dados pessoais entre pessoa de direito público e privado = ciência da ANPD + consentimento do titular

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

1. Nas hipóteses de dispensa de consentimento previstas nesta Lei; (ex. dados tornados manifestamente públicos pelo titular)
 2. Nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou (infos no site)
 3. Nas exceções constantes do § 1º do art. 26 desta Lei. (quando houver convênios, contratos cientificados à ANPD)
- Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação

Registros das Operações de Tratamento

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Publicação RIPD e Ações de Padrões e Boas Práticas

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a **publicação de relatórios** de impacto à proteção de dados pessoais e sugerir a **adoção de padrões e de boas práticas** para os tratamentos de dados pessoais pelo Poder Público.



Registros das Operações de Tratamento

Exemplo: em ação movida pela Defensorias Públicas da União e de SP, IDEC, Artigo 19 e Intervenções, para a produção de provas pelo Metrô de SP em relação à leitura facial de passageiros, o Poder Judiciário exigiu a apresentação do RIPD.

Link para mais informações: <https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/>

Seção II

Da responsabilidade

Em Caso de Violação

Art. 31. Quando houver **infração** a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com **medidas cabíveis** para fazer cessar a violação.



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



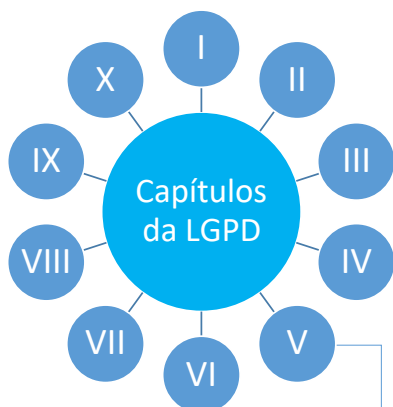
Módulo 6: Transferência Internacional de Dados



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Artigos 33 ao 36

Quando a transferência internacional é permitida?

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

1. Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei
2. 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
3. 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
4. Quando a transferência for necessária para a **proteção da vida** ou da incolumidade física do titular ou de terceiro
5. Quando a **autoridade nacional autorizar** a transferência
6. Quando a transferência resultar em compromisso assumido em acordo de **cooperação internacional**
7. 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



8. Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o carácter internacional da operação, distinguindo claramente esta de outras finalidades
9. Quando necessário para atender as 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 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

Nível de Proteção Exigido do País Estrangeiro

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

1. As normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional
2. A natureza dos dados
3. A observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei
4. A adoção de medidas de segurança previstas em regulamento
5. A existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais
6. Outras circunstâncias específicas relativas à transferência

Garantias Mínimas

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

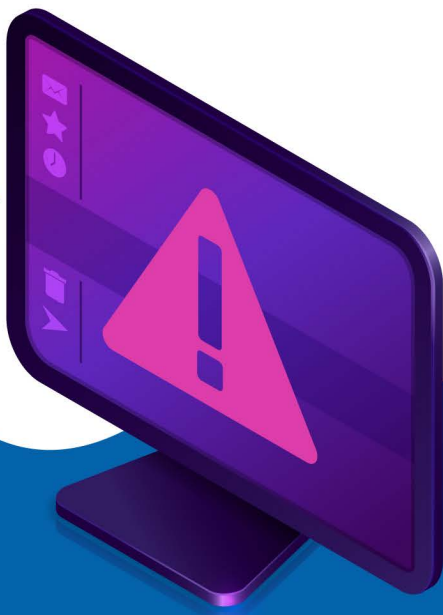
- § 1º. Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei
- § 2º. Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário
- § 3º. A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento
- § 4º. Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados
- § 5º. As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



Módulo 7: Agentes de Tratamento de Dados Pessoais



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO VI - OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Artigos 37 ao 45 Seção I - Do Controlador e do Operador – artigos 37 ao 40 Seção II - Do Encarregado pelo Tratamento de Dados Pessoais – artigo 41 Seção III - Da Responsabilidade e do Ressarcimento de Danos – artigos 42 ao 45

Lembrando

Art. 5º. Para os fins desta Lei, considera-se:

- IX - agentes de tratamento: o controlador e o operador



* Embora a LGPD defina como “Encarregado”, o termo “DPO” (advindo do GDPR) é popularmente referenciado por muitos profissionais de privacidade de dados do Brasil.

Seção I

Do Controlador e do Operador

# medida	tipo de medida	Medidas concretas	Tempo de conservação (se aplicável)	Tratamentos a que se aplica
M000a	ex: Medidas de proteção lógica	ex: antivírus, palavras passe com utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, testes		ex: T000, T005, T011
M000b	ex: Controlo de acessos às instalações	ex: apenas utilizadores com cartão nominal da entidade podem aceder		ex: todos os tratamentos
M000c	ex: Registo de log	ex: logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP	ex: 2 anos	ex: T002 a T010
M000d	ex: Encriptação dos dados	ex: site acessível através de https, utilização de TLS, pseudonimização do campo data de nascimento		ex: T004
M000e	ex: Salvaguarda dos dados	ex: backups diários, redundância, plano de disaster recovery com centro alternativo	ex: os backups são conservados por 3 anos	ex: T012
M001				
M002				
M003				
M004				
M005				
M006				
M007				
M008				
M009				
M010				
M011				
M012				
M013				
M014				
M015				
M016				
M017				
M018				
M019				
M020				
M021				
M022				
M023				
M024				
M025				

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

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
 - A análise do controlador com relação a medidas
 - Salvaguardas e mecanismos de mitigação de risco adotados
- Software open source da CNIL: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>
- Versões para Mac, Windows, Linux, front end, back end



PIA - Privacy Impact Assessment

Version v2.2.1

Analise de Impacto da Proteção de Dados
Privacy Impact Assessment

PAINEL

MODELOS DE PIA

Ferramentas

Teste

CONTEXTO

- Visão geral
- Dados, processos e ativos de su...

PRINCÍPIOS FUNDAMENTAIS

- Proporcionalidade e necessidade
- Controles para proteger os direit...

RISCOS

- Medidas planejadas ou existentes
- Acesso ilegítimo dos dados
- Modificação indesejada dos dad...
- Desaparecimento de dados
- Visão geral dos riscos

VALIDAÇÃO

- Mapeamento dos riscos
- Plano de ação
- DPO e opiniões de partes interes...

Validar análise PIA

ANEXOS

+ Adicionar

Contexto

Esta seção fornece uma visão clara do(s) tratamento(s) de dados pessoais em questão.

VISÃO GERAL

Esta seção permite identificar e apresentar o objeto de estudo.

Qual é a finalidade de tratamento considerada no âmbito da análise?

Descreva a finalidade de tratamento, incluindo nome, objetivos e benefícios dessa finalidade, contexto de utilização, etc.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

Descreva as responsabilidades de todos os intervenientes envolvidos na finalidade de tratamento, identificando a entidade que atua como responsável pelo tratamento, entidades subcontratadas que tratem estes dados, terceiros autorizados, entre outros.

Responsável pelo tratamento é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras (responsáveis conjuntos), determina as finalidades e os meios de tratamento de dados pessoais.

No caso de existirem responsáveis conjuntos pelo tratamento, estes

Quais são as normas aplicáveis à finalidade de tratamento?

Para esta finalidade de tratamento identifique as normas seguidas pela organização, especialmente códigos de conduta aprovados, certificações de proteção de dados e/ou segurança da informação, cláusulas de subcontratação com indicação expressa da forma de utilização dos dados, entre outros.

Base de conhecimento

Princípio

Descrição do tratamento

Definição

Responsável pelo tratamento

Definição

Subcontratante

Dados, processos e ativos de suporte >

Informação PIA

PIA

Análise de Pele com IA

Nome do autor

Dono do Projeto

Nome do assessor

Assessor do Dono do Projeto

Nome do validador

Matheus Silva (DPO)

Data de criação

04/09/2019

Nome do DPO

Matheus Silva

Modificação indesejada dos dados

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?

Discriminação social em decorrência do tipo de pele, Uso de email para propaganda indesejada

Quais são as principais ameaças que poderiam levar ao risco?

Colaboradores desonestos, Colaboradores mal treinados, Cracker

equipamentos, Falhas em estruturas físicas, Falhas de comunicações

Quais são as fontes de risco?

Humanas intencionais, Humanas não intencionais

Quais são os controles identificados que poderiam mitigar o risco?

Cifragem, Anonimização, Controle de acesso

Gerenciamento de violações de dados pessoais

Como estimas a gravidade do risco, se ocorrer?

Insignificante

Insignificante

Insignificante

Insignificante

Insignificante

Insignificante

Insignificante

Insignificante: os titulares dos dados não serão afetados

Visão geral dos riscos

Impactos potenciais

Divulgação de nomes

Divulgação de emails

Uso de email para propagand...

Discriminação social em dec...

Envio de material não condi...

Não recebimento de informaç...

Não recebimento de publicid...

Acesso ilegítimo dos dados

Gravidade : Significativo

Probabilidade : Limitado

Ameaças

Colaboradores mal treinados

Colaboradores negligentes

Cracker

Colaboradores desonestos

Falhas em estruturas físicas

Falha ou defeito de equipam...

Falta de comunicações

Problemas de/com software

Modificação indesejada dos dados

Gravidade : Insignificante

Probabilidade : Insignificante

Operador x Controlador

Art. 39. O operador deverá realizar o tratamento **segundo as instruções fornecidas pelo controlador**, que verificará a observância das próprias instruções e das normas sobre a matéria.



Outras Obrigações dos Agentes de Tratamento

- Informação e transparência
- Privacy by Design
- Contratos entre Controlador e Operador
- Medidas de Segurança
- Notificações em caso de violação de dados pessoais

Padrões de Interoperabilidade

Art. 40. A autoridade nacional poderá dispor sobre **padrões de interoperabilidade** para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.



Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Será abordado no próximo módulo

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Reparação de Danos

Art. 42. 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 à legislação de proteção de dados pessoais, é obrigado a repará-lo.

- § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
 1. O operador responde solidariamente pelos danos causados pelo tratamento quando **descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador**, salvo nos casos de exclusão previstos no art. 43 desta Lei
 2. Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei
- § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa
- § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente
- § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso

Quando agentes não serão responsabilizados?

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

1. Que não realizaram o tratamento de dados pessoais que lhes é atribuído
2. Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados
3. Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro

Quando o tratamento é considerado irregular?

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

1. O modo pelo qual é realizado;
 2. O resultado e os riscos que razoavelmente dele se esperam;
 3. As técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
- **Parágrafo único.** Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano

Violação do Direito do Titular

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



Módulo 8: Encarregado (ou DPO)



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



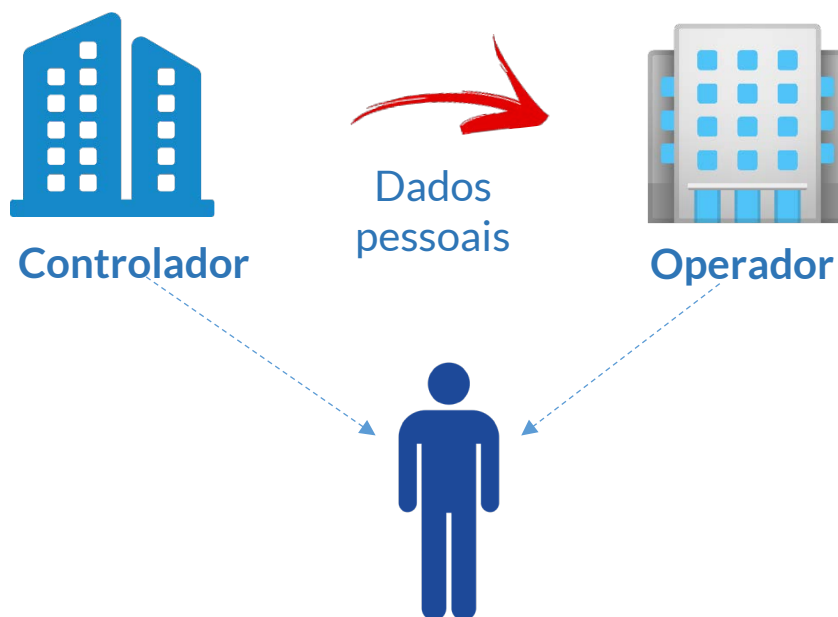
CAPÍTULO VI - OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Artigos 37 ao 45 Seção I - Do Controlador e do Operador – artigos 37 ao 40 Seção II - Do Encarregado pelo Tratamento de Dados Pessoais – artigo 41 Seção III - Da Responsabilidade e do Ressarcimento de Danos – artigos 42 ao 45

Lembrando

Art. 5º Para os fins desta Lei, considera-se:

- **VIII - encarregado:** 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)



Dica Prática!

Estudo de Caso Público: ANPPD.org

O Portal da ANPPD centralizado e modificado o maior banco de dados de Profissionais de Privacidade do Brasil, em que é possível buscar pelo Encarregado (DPO) desejado e que já foi avaliado pela ANPPD, que é a maior associação de classe da América Latina. Muitas empresas no estão utilizando essa pré-avaliação em seus processos seletivos bem como os profissionais se oferecendo ao mercado.

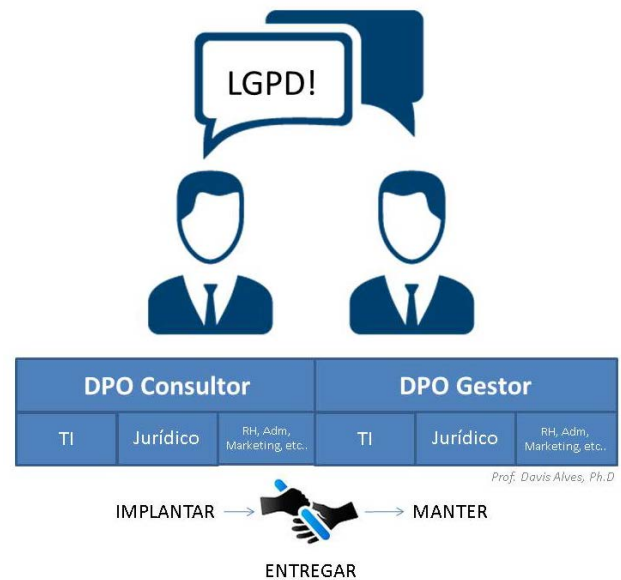
A certificação LGPDF é reconhecida e aceita pela ANPPD para ingresso.



Nomeação de um Encarregado

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

- § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador
- Outros termos como “Oficial de Proteção de Dados” também são referenciados
- Entre as diferenças técnicas entre o “Encarregado” e o “DPO”, destaca-se que enquanto o DPO possui um caráter mais técnico, o Encarregado na LGPD esta positivado como um “Comunicador”. Entretanto, mesmo assim, popularmente o termo “DPO” é popularmente referenciado por muitos profissionais de privacidade de dados do Brasil. *Nesse material segue equivalente ao termo popular*



Fonte: Davis Alves, Ph.D

#LGPDNews! – Fique por dentro!

Em 29 de julho de 2021 foi incluída e reconhecida oficialmente a ocupação de DPO/Encarregado pelo Tratamento de Dados na CBO – Classificação Brasileira de Ocupações que terá início em 2022. As reuniões, entrevistas e detalhamento da nova profissão, estavam sendo discutidas desde o início de 2021 entre a FIPE/CBO do Ministério da Economia (atual Ministério do Trabalho), e a ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados através da presidência e membros participantes que já atuam como DPO na prática.

LGPD News

ANPPD
Associação Nacional dos Profissionais de Privacidade de Dados

CLASSIFICAÇÃO BRASILEIRA DE OCUPAÇÕES

DPO/Encarregado foi reconhecido no Brasil!

A ANPPD® finalizou a reunião com a equipe da CBO – Classificação Brasileira de Ocupações para reconhecimento do DPO/Encarregado pelo Tratamento de Dados no Brasil

Membros participantes:

Daniel Carnáuba, DPO ANPPD/SP	Rodrigo Muniz, DPO ANPPD/MG
Juliana Costa, DPO ANPPD/SP	André Nunes, DPO ANPPD/DF
Dr. Davis Alves, DPO Presidente da ANPPD	

LGPD CONNECT 2021
#ConformidadeJá

anppd.org/noticias

Membros ANPPD & Ministério do Trabalho (CBO)
29 de julho de 2021

Fonte: https://www.linkedin.com/posts/anppd_lgpdnews-anppdmerepresenta-lgpdconnect2021-activity-6826842880909352960-tKk2

Quem pode ser um encarregado?

Inicialmente, o texto original da LGPD previa que o encarregado seria “pessoa natural”. No entanto, a palavra “natural” foi suprimida pela Medida Provisória nº 869 e esta alteração foi confirmada pela Lei 13.853/2019. Logo, podemos assumir:



Atividades de um Encarregado

Art. 41.

- § 2º As atividades do encarregado consistem em:
 1. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências
 2. Receber comunicações da autoridade nacional e adotar providências
 3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais
 4. 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

Um DPO Pode Atender a Várias Organizações

- Tanto a LGPD como o GDPR permitem que um DPO possa atender a várias organizações
- Importante que ele esteja facilmente acessível por todas as organizações que atende



Qualificações Recomendadas

Quais conhecimentos e habilidades um DPO precisa ter?

Qualificações Recomendadas Para um DPO

- O “mito” do DPO jurídico e do DPO técnico
- Não há separação entre “jurídico” e “técnico” – há a proteção de dados. O profissional deve ter conhecimentos sólidos a respeito das duas áreas, além de conhecer o negócio
- Exemplos de multas na UE em 2019 por falha em cada um dos aspectos acima:
 - Infrações ao art. 6º (bases legais): 27 multas, total 19.257.894 euros
 - Infrações ao art. 32º (segurança): 22 multas, total 6.526.027 euros
 - Excluídos: multas ao Marriott International (110,4M) e à British Airways (204,6M segurança) e à Google (50M bases legais) por serem “pontos fora da curva” (casos excepcionais) – Marriott e BA ainda em julgamento, Google – decisão já final

O GDPR e a LGPD não estabelecem as qualificações mínimas exigidas para sua atuação. Porém há certos atributos e conhecimentos recomendados para este papel:



Fonte: adaptado de EU General Data Protection Regulation (RGPD). An Implementation and Compliance Guide, ITGP

Onde estão os DPOs no mundo?



CONNECT
with other privacy pros from around the world.

20 iapp

✓ Following

IAPP - International Association of Privacy Professionals

Non-profit Organization Management
Portsmouth, NH • 69.746 followers

Your comprehensive global information privacy community and resource

IAPP.org



EADPP european association of data protection professionals

EADPP

✓ Following

EADPP - European Association of Data Protection Professionals

Non-profit Organization Management
Maastricht, Limburg • 4.339 followers

EADPP.eu



APDPO PORTUGAL
Associação dos Profissionais de Proteção e de Segurança de Dados

APDPO

✓ Following

APDPO

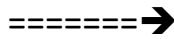
Non-profit Organization Management
Lisboa, Lisboa • 359 followers

Associação Portuguesa de Data Protection Officers, uma associação profissional que representa indivíduos ou organizações

APDPO.pt



ANPPD.org




ANPPD ENCARGADOS | DATA PROTECTION OFFICERS - DPOs DO BRASIL

ANPPD

Edit page

ANPPD® - Associação Nacional dos Profissionais de Privacidade...

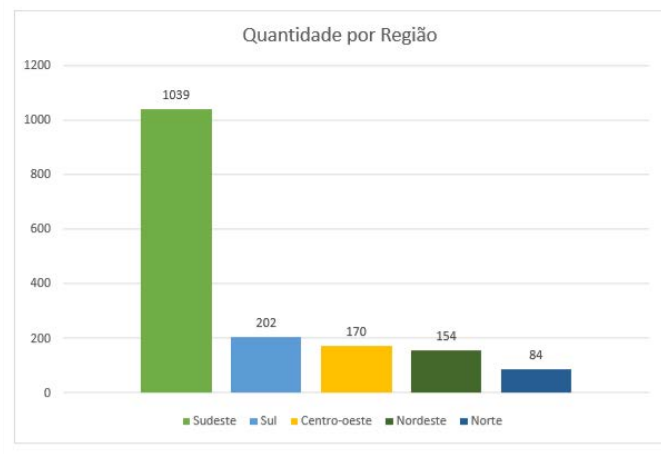
Government Relations • Brasil • 8.368 followers

Encarregados | Data Protection Officers - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados - 13.709/2018 🇧🇷

Associações de Profissionais de Privacidade de Dados

Perfil do DPO no Brasil (ANPPD, 2020)

Profissionais de Privacidade de Dados no Brasil




ANPPD ENCARGADOS | DATA PROTECTION OFFICERS - DPOs DO BRASIL

ANPPD

Edit page

ANPPD® - Associação Nacional dos Profissionais de Privacidade...

Government Relations • Brasil • 8.368 followers

Encarregados | Data Protection Officers - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados - 13.709/2018 🇧🇷

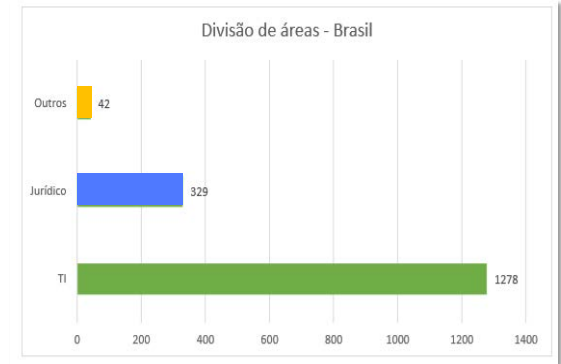
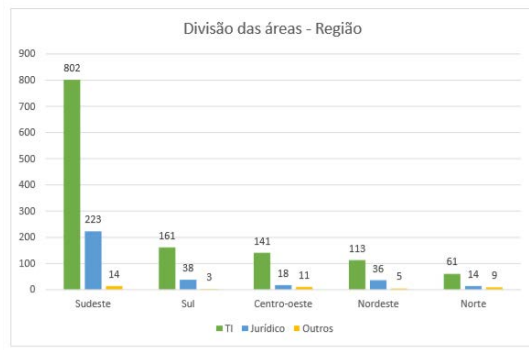
* Mais de 30 mil seguidores no LinkedIn em 2021

1649 aprovados como Membros ANPPD em 2020, e mais de 10.000 em 2021.



LEGENDA

- Comitê Diretivo
- Comitê Científico
- Comitê de Conteúdo
- Comitê Público
- Comitê de Segurança
- Comitê de Imprensa
- Comitê de Eventos
- Comitê Jurídico
- ★ Membro de Honra

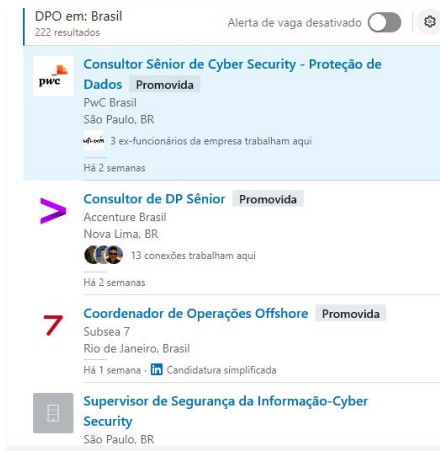
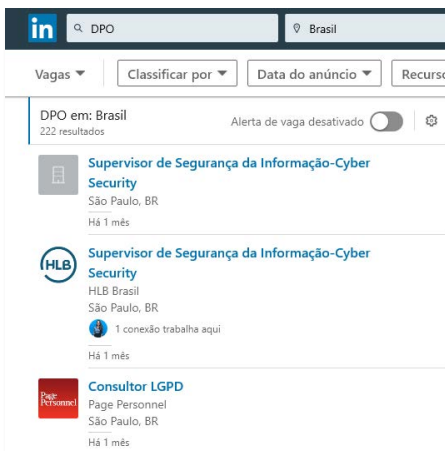


DPOs no Brasil
1649 aprovados como Membros ANPPD em 2020, e mais de 10.000 em 2021

anppd.org

Vagas para DPOs, Encarregados, Oficiais de Proteção de Dados

- Média salarial DPO:
 - Consultor: R\$ 350,00 à R\$ 550,00 p/hora – (referência OAB, Tabela IBAPE)
 - Gestor interno: R\$ 8.000,00 à R\$ 20.000,00 – (referência à GDPR in Numbers)



04/05/2020

17 Conhecimentos Específicos para um DPO/Encarregado

De acordo com o esquema de certificação de DPO proposto pelo CNIL (Autoridade da França), existem 17 conhecimentos específicos que um DPO precisa ter:

1. Compreender e entender os **princípios da legalidade do processamento**, limitação de finalidades, minimização de dados, exatidão dos dados, retenção limitada de dados, integridade, confidencialidade e responsabilidade
2. Saber como identificar a **base legal** para um tratamento
3. Saber como determinar as **medidas apropriadas** e o conteúdo das informações a serem fornecidas aos titulares
4. Saber como estabelecer **procedimentos** para receber e gerenciar **solicitações** para o exercício dos direitos dos titulares
5. Conhecer a estrutura legal relacionada à **terceirização** do processamento de dados pessoais

6. Saber como identificar a existência de **transferências de dados** fora do país e como determinar os instrumentos legais de transferência que podem ser usados
7. Saber como desenvolver e implementar uma **política ou regras internas** de proteção de dados
8. Saber como organizar e participar de **auditorias** de proteção de dados
9. Estar familiarizado com o conteúdo do **registro de atividades de processamento**, a categoria do registro de atividades de processamento e a documentação de violações de dados, bem como a documentação necessária para comprovar a conformidade com os regulamentos de proteção de dados
10. Saber como identificar **medidas de proteção de dados a partir do design e, por padrão**, adaptado aos riscos e à natureza das operações de processamento
11. Saber participar da **identificação de medidas de segurança apropriadas aos riscos** e à natureza das operações de processamento
12. Saber como **identificar violações de dados** pessoais que exigem notificação à autoridade supervisora e aquelas que exigem comunicação com os titulares dos dados
13. Saber se é necessário ou não realizar uma **avaliação de impacto na proteção de dados (DPIA)** e saber como verificar sua implementação
14. Fornecer **consultoria sobre avaliação de impacto na proteção de dados** (especialmente sobre metodologia, possível terceirização, medidas técnicas e organizacionais a serem adotadas)
15. Saber como **gerenciar as relações com as autoridades de supervisão**, respondendo às solicitações e facilitando a ação (investigação de reclamações e controles em particular)
16. Ser capaz de desenvolver, implementar e oferecer **programas de treinamento e conscientização** para a equipe e a gerência sênior sobre proteção de dados
17. Saber como garantir a **rastreabilidade de suas atividades**, principalmente com a ajuda de ferramentas de monitoramento ou relatório anual

Fonte: <https://www.legifrance.gouv.fr/>

Alguns Regulamentos que um DPO no Brasil Precisa Conhecer



Indispensável conhecer sobre os prazos de guarda de documentos fiscais, comerciais, trabalhistas e previdenciários conforme legislação aplicável.

[Consulte aqui](#)

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



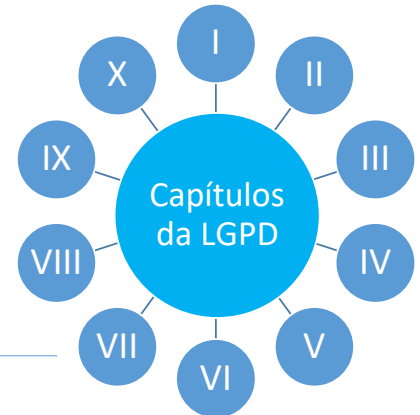
Módulo 9: Segurança e Boas Práticas - Teórica & Prática



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?



CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS

Artigos 46 ao 51

Seção I - Da Segurança e do Sigilo de Dados – artigos 46 ao 49

Seção II - Das Boas Práticas e da Governança – artigos 50 e 51

Seção I

Da Segurança e do Sigilo de Dados

Adoção de Medidas

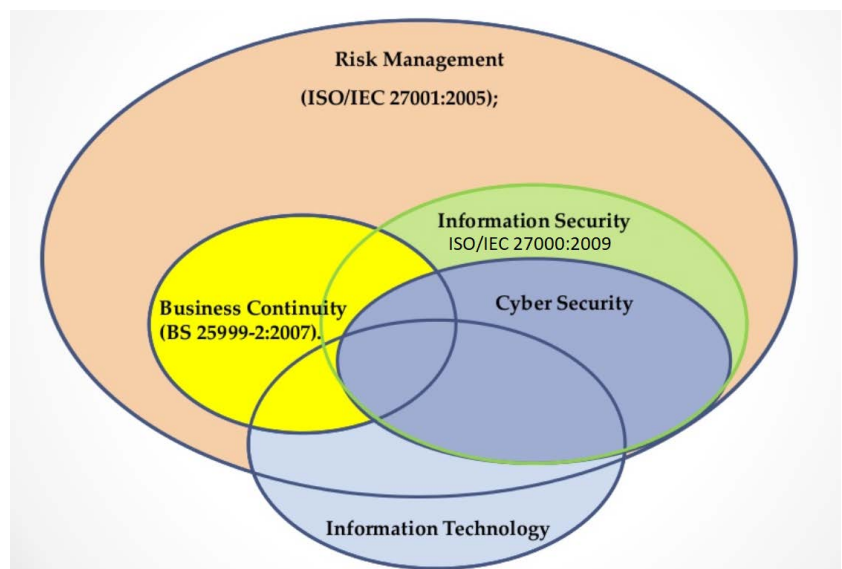
Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

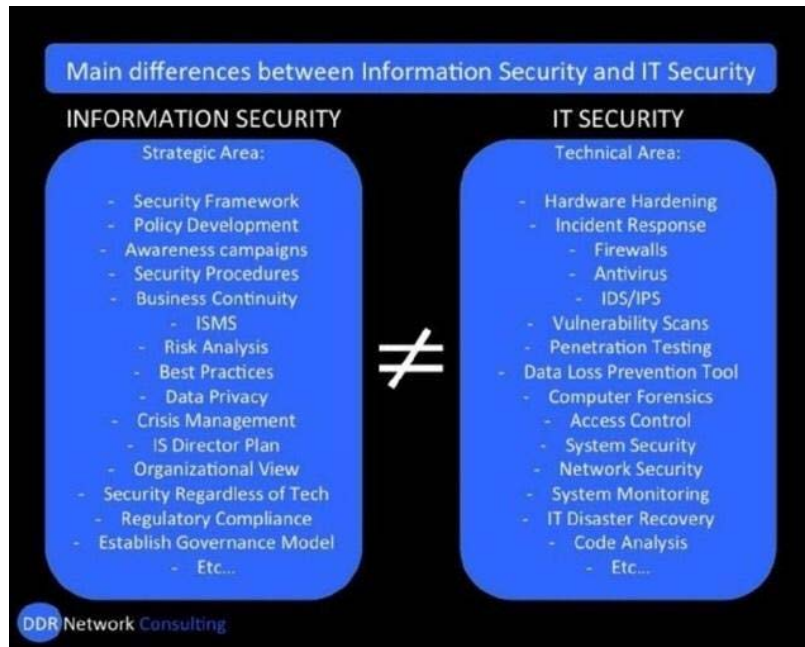
Segurança da Informação

3 Tipos de Medidas de Segurança:

- SEGURANÇA FÍSICA
- SEGURANÇA TÉCNICA
- SEGURANÇA ORGANIZACIONAL



Fonte: 51sec.org (2020)



Comunicação do Incidente de Segurança

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.

- § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
 1. A descrição da natureza dos dados pessoais afetados
 2. As informações sobre os titulares envolvidos
 3. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial
 4. Os riscos relacionados ao incidente
 5. Os motivos da demora, no caso de a comunicação não ter sido imediata
 6. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Das Boas Práticas e da Governança



Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam 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.

Art. 50. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

- I - implementar programa de governança em privacidade que, no mínimo:
 - a) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais
 - b) Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta
 - c) Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados
 - d) Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade
 - e) Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular
 - f) Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos
 - g) Conte com planos de resposta a incidentes e remediação
 - h) Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas

Objetivos de Controles da ISO 27001



- Implantação do SGSI
- Políticas de Segurança
- Organização da Informação
- Gestão de Ativos
- Controle de Acessos
- Criptografia
- Segurança Física e Ambiental
- Segurança das Operações
- Aquisição de Sistemas, Desenvolvimento e Manutenção
- Transferência de Informações
- Relação com Fornecedores
- Gestão de Incidentes de Segurança
- Continuidade do Negócio
- Cumprimento de requisitos legais e contratuais

Cyber-ataques em Tempo Real



<https://threatmap.checkpoint.com/>

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS LGPD™



Já tive dados pessoais vazados?

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

454	9,760,722,439	112,905	135,168,575
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

- 772,904,991 Collection #1 accounts
- 763,117,241 Verifications.io accounts
- 711,477,622 Onliner Spambot accounts
- 622,161,052 Data Enrichment Exposure From

Recently added breaches

- 25,692,862 Mathway accounts
- 3,589,795 Zoomcar accounts
- 68,693,853 Lead Hunter accounts
- 9,705,172 Wishbone (2020) accounts

<https://haveibeenpwned.com/>

Para onde vão os dados pessoais vazados?

PASTEBIN GO PRO API TOOLS FAQ DEALS + paste

New Paste

Optional Paste Settings

Syntax Highlighting: None

Paste Expiration: Never

Paste Exposure: Public

Folder:

Paste Name / Title:

Create New Paste

Hello Guest
Sign Up or Login

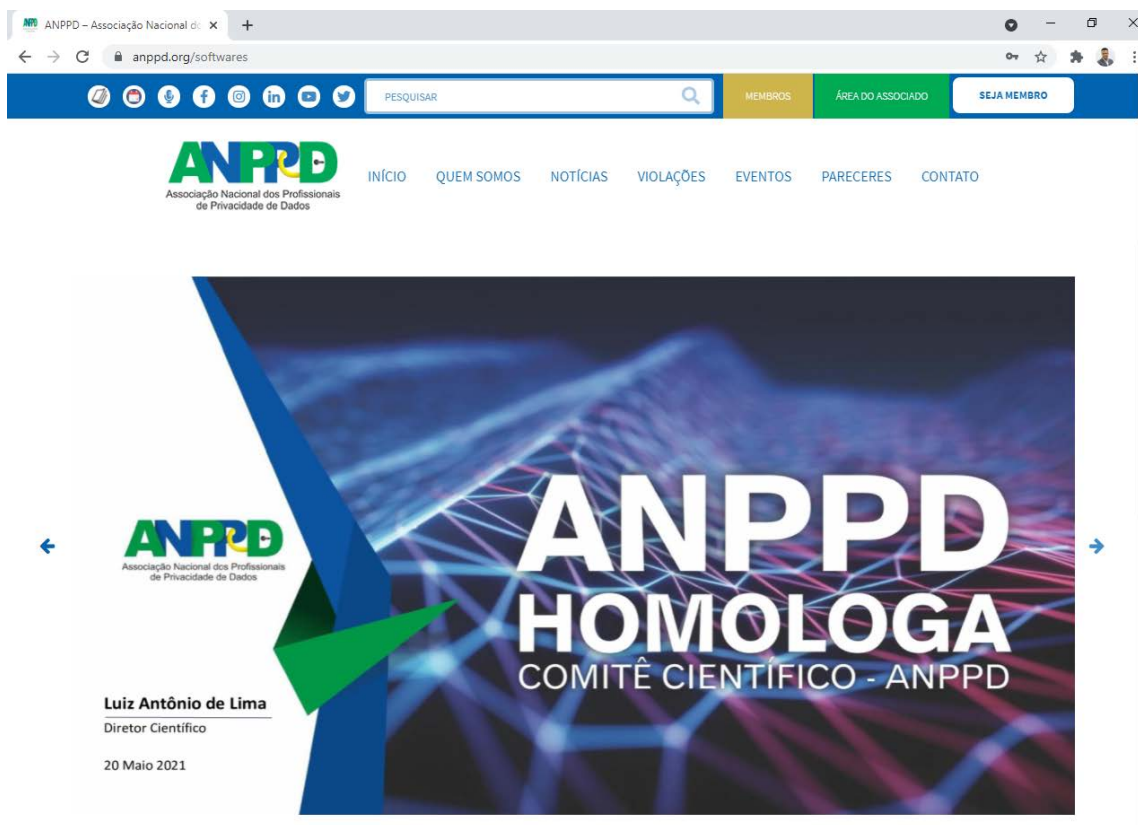
Sign in with Facebook
Sign in with Twitter
Sign in with Google

<https://pastebin.com/>

Onde buscar ferramentas para LGPD?

O Programa de Homologação de Software da ANPPD é um processo desenvolvido pelo Comitê Científico reconhecido internacionalmente nas revistas científicas: “KES - Knowledge-Based and Intelligent Information & Engineering Systems: Elsevier's Procedia Computer Science Open Access Journal, Science Direct; Web of Science, Scopus”. Este processo verifica através de evidências geradas pelo software com aderência da empresa à LGPD, GDPR, ISO-27001, ISO-27701 e outros indicadores. Após todo o processo a ferramenta recebe a CHANCELA/Selo que é ANPPD Ouro, ANPPD Prata ou ANPPD Bronze, dependendo do resultado verificado.

Este selo é entregue juntamente com o Certificado de Homologação, remoto ou presencialmente na sede da empresa proprietária da ferramenta. As evidências de conformidade são passíveis de verificação pública na *Software House* e registradas na ANPPD, respeitando todos os segredos industriais. O Programa de Homologação da ANPPD é conduzido por mestres e doutores especialistas em LGPD/GDPR, e utiliza as metodologias Científicas: Design Science Research (HEVNER et al. 2007) e estudo de caso (GIL, 2008)., sendo dividido em 3 Fases de auditorias: a) Análise Documental, b) Entrevistas e c) Observação Direta (GIL, 2008). Este processo de homologação é um serviço da ANPPD para a sociedade com o objetivo mostrar ao mercado as melhores opções de softwares cientificamente verificadas.



<https://anppd.org/software>

Por onde começar a Política de Segurança?

Download PDF: https://www.linkedin.com/posts/anppd_projeto-de-implanta%C3%A7%C3%A3o-da-iso-2700127701-activity-6630495127473266688-pxL7/



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



Módulo 10: Sanções Administrativas



LGPDF™ Versão 092021

CertiProf®

Em qual parte da lei estamos?

CAPÍTULO VIII – DA FISCALIZAÇÃO

Seção I - Das Sanções Administrativas – artigos 52 ao 54



Responsabilização

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.

- A descrição da natureza dos dados pessoais afetados
- As informações sobre os titulares envolvidos
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dados
- Os riscos relacionados ao incidente
- Os motivos da demora, no caso de a comunicação não ter sido imediata
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo



Aplicação de Sanções Administrativas

-> Quem aplicará? Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Sanções Previstas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

- 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. Publicização 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 ([Incluído pela Lei nº 13.853, de 2019](#))
- 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 ([Incluído pela Lei nº 13.853, de 2019](#))
- XII. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Critérios para Aplicação Das Sanções

Art. 52. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- I. A gravidade e a natureza das infrações e dos direitos pessoais afetados
- II. A boa-fé do infrator
- III. A vantagem auferida ou pretendida pelo infrator
- IV. A condição econômica do infrator
- V. A reincidência
- VI. O grau do dano
- VII. A cooperação do infrator
- VIII. A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei
- IX. A adoção de política de boas práticas e governança
- X. A pronta adoção de medidas corretivas
- XI. A proporcionalidade entre a gravidade da falta e a intensidade da sanção

Fiscalização por Outros Órgãos

Outros órgãos já têm atuado como fiscalizadoras e com aplicação de sanções:

- PROCON e a ANATEL possibilitam a oposição quanto ao recebimento de ligações de telemarketing - <https://www.naomeperturbe.com.br/>
- O Ministério Público tem multado se tal procedimento não é respeitado pelas operadoras - <https://www.mpmg.mp.br/comunicacao/noticias/vivo-devera-pagar-multa-de-r-10-4-milhoes-por-desrespeito-ao-sistema-de-bloqueio-de-telemarketing-do-mpmg.htm>
- Ação movida pela Defensorias Públicas da União e de SP, IDEC, Artigo 19 e Intervezes, para a produção de provas pelo Metrô de SP em relação à leitura facial de passageiros, o Poder Judiciário exigiu a apresentação do RIPD. <https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/>

Destino das Arrecadações

Art. 52. § 5º. O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 19.

FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS



Módulo 11: Autoridade Nacional de Proteção de Dados (ANPD)



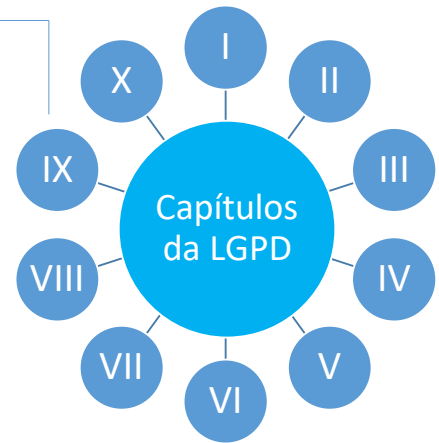
LGPDF™ Versão 092021

CertiProf®

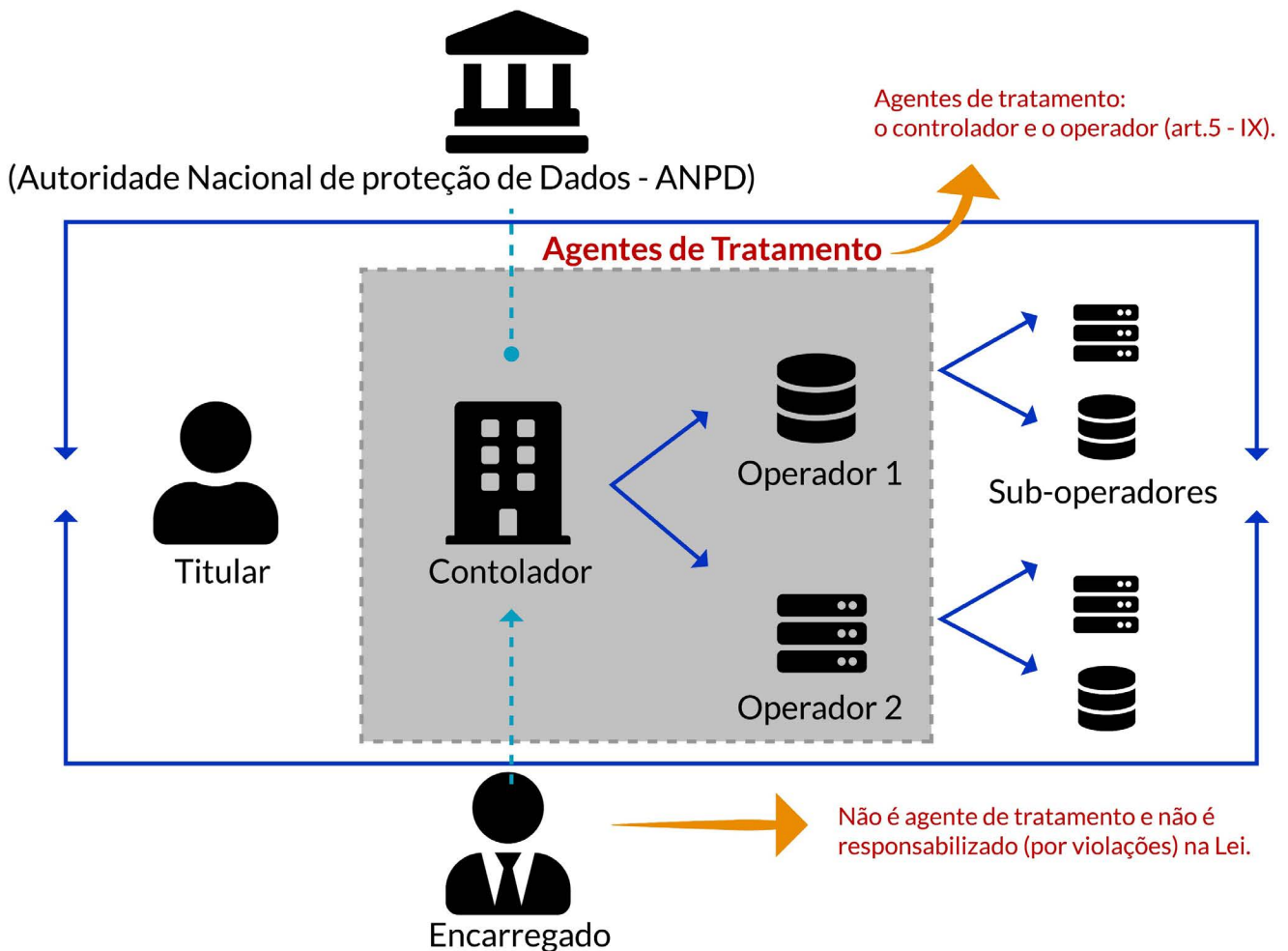
Em qual parte da lei estamos?

CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

- Artigos 55-A ao 58-B
- Seção I - Da Autoridade Nacional de Proteção de Dados (ANPD) - artigos 55-A ao 55-L
- Seção II - Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade - artigos 58- A ao 58-B



Autoridade Nacional de Proteção de Dados - ANPD



Criação da ANPD

Autoridade Nacional de Proteção de Dados (ANPD) - Art. 55-A

- Órgão da administração pública federal, integrante da Presidência da República
- § 1º. A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República
- § 2º. A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD
- § 3º. O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD.

Composição da ANPD

A ANPD é composta de:

- **Conselho Diretor**, órgão máximo de direção (diretor presidente e 5 outros diretores)
- **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade** (23 membros, que não serão remunerados por suas atividades, sendo representantes: da sociedade civil, de entidades representativas, do Senado Federal, Câmara dos Deputados e outros)
- **Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; e unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei**

(Art. 55-C)

Problemática

Por não ter LGPD vigente e ANPD estruturada, o Brasil é classificado como destino inadequado em termos de proteção de dados pessoais.

<https://www.cnil.fr/en/data-protection-around-the-world>

Atribuições da ANPD

Atribuições

- **Poderes de investigação.** Ex: para realizar auditorias de proteção de dados, para notificar o controlador ou operador de uma suposta violação
- **Poderes corretivos.** Ex: ao emitir repreensões, ordenar a comunicação de uma violação de dados pessoais a um titular de dados, cancelar uma certificação, impor sanções
- **Poderes consultivos.** Ex: para adotar cláusulas contratuais padrão, para emitir certificações, acreditar organismos certificadores

-> Art. 55-B. É assegurada autonomia técnica e decisória à ANPD.

Competências da ANPD

Compete à ANPD (Art. 55-J):

1. Zelar pela proteção dos dados pessoais, nos termos da legislação
2. 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
3. **Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade**
4. 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
5. **Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação**
6. **Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança**
7. Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade
8. **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**
9. Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional
-

Cooperação da ANPD com Outros Órgãos

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

Relacionamento ANPD

Audiência pública no STF ref. ADC 51, que debateu, em janeiro/2020, sobre o acordo internacional entre Brasil e EUA sobre o fornecimento de provas e dados por empresas nos EUA para investigações criminais do Brasil.

Acordo de Assistência Judiciária em Matéria Penal BR e EUA (MLAT):

- http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm#:~:text=Promulga%20o%20Acordo%20de%20Assist%C3%Aancia,15%20de%20fevereiro%20de%202001.
- <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=436573>



Conselho Nacional de Proteção de Dados (CNPd)

No dia 09 de agosto de 2021 o Presidente da República, Jair Bolsonaro, nomeou os membros do CNPD.

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: ([Incluído pela Lei nº 13.853, de 2019](#))

- I. Propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; ([Incluído pela Lei nº 13.853, de 2019](#))
- II. Elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; ([Incluído pela Lei nº 13.853, de 2019](#))
- III. Sugerir ações a serem realizadas pela ANPD; ([Incluído pela Lei nº 13.853, de 2019](#))
- IV. Elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e ([Incluído pela Lei nº 13.853, de 2019](#))
- V. Disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população ([Incluído pela Lei nº 13.853, de 2019](#))

DECRETOS DE 9 DE AGOSTO DE 2021

< Voltar

Compartilhe

VERSÃO CERTIFICADA

DIÁRIO COMPLETO

IMPRESSÃO



DIÁRIO OFICIAL DA UNIÃO

Publicado em: 10/08/2021 | Edição: 150 | Seção: 2 | Página: 1

Órgão: Atos do Poder Executivo

CASA CIVIL

DECRETOS DE 9 DE AGOSTO DE 2021

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, inciso VI, alínea "a", da Constituição, e tendo em vista o disposto no art. 58-A da Lei nº 13.709, de 14 de agosto de 2018, e no art. 15 do Decreto nº 10.474, de 26 de agosto de 2020, resolve:

DESIGNAR

os seguintes membros para compor o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

Confira **AQUI** a lista dos Membros do CNPD:

[DECRETOS DE 9 DE AGOSTO DE 2021 - DECRETOS DE 9 DE AGOSTO DE 2021 - DOU - Imprensa Nacional \(in.gov.br\)](#)

Fiscalização por Outros Órgãos

Outros órgãos já têm atuado como fiscalizadoras e com aplicação de sanções:

- PROCON e a ANATEL possibilitam a oposição quanto ao recebimento de ligações de telemarketing - <https://www.naomeperturbe.com.br/>
- O Ministério Público tem multado se tal procedimento não é respeitado pelas operadoras - <https://www.mpmg.mp.br/comunicacao/noticias/vivo-devera-pagar-multa-de-r-10-4-milhoes-por-desrespeito-ao-sistema-de-bloqueio-de-telemarketing-do-mpmg.htm>
- Ação movida pela Defensorias Públicas da União e de SP, IDEC, Artigo 19 e Intervozes, para a produção de provas pelo Metrô de SP em relação à leitura facial de passageiros, o Poder Judiciário exigiu a apresentação do RIPD. <https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/>

Destino das Arrecadações

Art. 52. § 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 19.

Referências

Literatura bibliográfica

- LGPD (2018) – Lei 13.709/2018 - Geral de Proteção de Dados Pessoais. Presidência da República do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- ANPD (2020) – Decreto 10.474.2020 – Estrutura Regimental da Autoridade Nacional de Proteção de Dados. Presidência da República do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- SGD/ME (2020) – Publicação 16/06/2021 - Guia de Boas Práticas da Lei Geral de Proteção de Dados. Secretaria de Governo Digital do Ministério da Economia do Brasil. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd>
- Encarregados | DPO (2021) – Livro: Encarregados | Data Protection Officer. Davis Alves & Adrienne Lima. Editora Haikai. Disponível em: https://www.amazon.com.br/Encarregados-MS-c-Davis-Alves-Adrienne/dp/6586334888/ref=sr_1_8?_mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=DPO&qid=1627076210&s=books&sr=1-8&ufe=app_do%3Aamzn1.fos.fcd6d665-32ba-4479-9f21-b774e276a678
- Proteção de Dados Pessoais (2020) – Livro: Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD. Patricia Peck Pinheiro. Editora Saraiva. Disponível em: https://www.amazon.com.br/Prote%C3%A7%C3%A3o-Dados-Pessoais-Coment%C3%A1rios-13-709/dp/8553617483/ref=sr_1_3?_mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=dpo+PECK&qid=1627076355&s=books&sr=1-3-catcorr

Referências técnicas e acadêmicas

- ABNT NBR ISO-27001 (2013) – Norma técnica – Sistema de Gestão de Segurança da Informação - Requisitos. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306580>
- ABNT NBR ISO-27002 (2013) – Norma técnica – Sistema de Gestão de Segurança da Informação – Código de Práticas. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306582>
- ABNT NBR ISO-27701 (2020) – Norma técnica – Sistema de Gestão da Privacidade da Informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=437612>
- ABNT NBR ISO-27701 (2020) – Norma técnica – Sistema de Gestão da Privacidade da Informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=437612>



FUNDAMENTOS NA LEI GERAL DE PROTEÇÃO DE DADOS

Siga-nos, entre em contato!



www.certiprof.com

CERTIPROF® é uma marca registrada da CertiProf,
LLC nos Estados Unidos e / ou outros países.

CertiProf®