

# Privacidade e Proteção de Dados

Luiz Felipe Vieira de Siqueira

# Tópicos de Privacidade e Proteção de Dados Pessoais

# Luiz Felipe Vieira de Siqueira

- Advogado
- Sócio Privacy Point
- DPO EXIN
- Mestre em Direito Empresarial
- Doutorando UFMG
- Professor de Pós Graduação
- Linkedin:  
<https://www.linkedin.com/in/luizfelipesiqueira/>



**LUIZ FELIPE SIQUEIRA**  
ADVOGADO

**privacypoint**

- 📱 (31) 98589-0609
- ✉️ siqueira@privacypoint.com.br
- 🌐 privacypoint.com.br
- 📍 Rua Fernandes Tourinho,  
929/12º andar – Bairro Lourdes  
Belo Horizonte - MG  
CEP: 30.112-003

# Marco Teórico – Right to Privacy

- “The Right to Privacy”
- Warren and Brandeis
- Harvard Law Review, Vol. IV  
December 15, 1890 No. 5

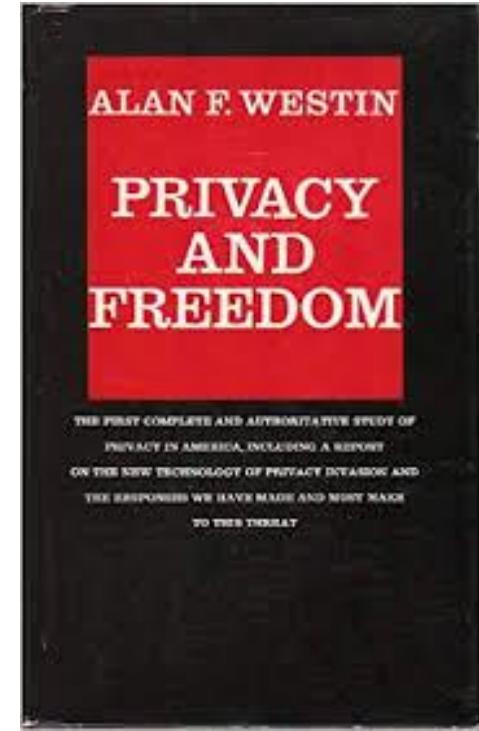


Fonte: Harvard Law Review

# Marco Teórico – Alan Westin

## Privacidade – Vida Privada

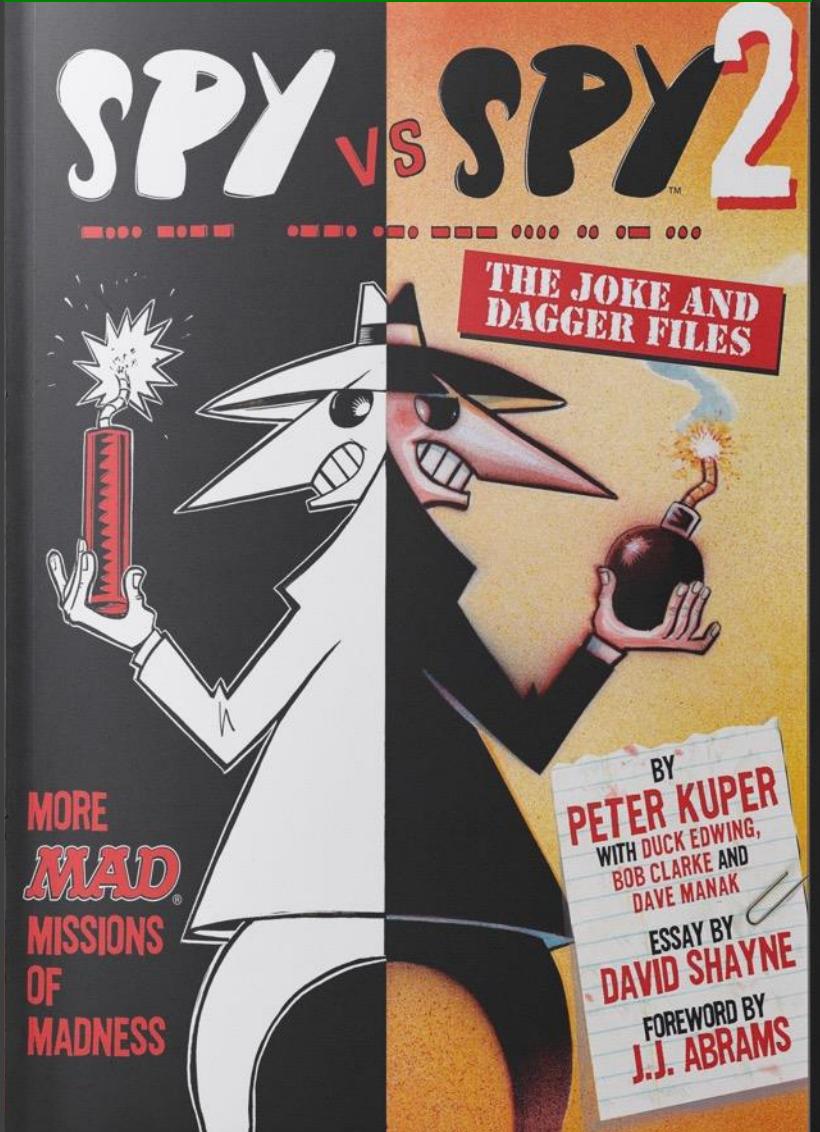
Alan Westin em sua obra “Privacy and Freedom” (1967) mostra a **natureza biológica** da privacidade. Ele demonstra que virtualmente toda espécie animal busca períodos de reclusão individual ou de intimidade em pequenos grupos.



Fonte: <https://www.amazon.com.br/Privacy-Freedom-Alan-Westin/dp/1935439979>

# Alan TURING





# Spy vs Spy

# Snowden

MARCO CIVIL DA INTERNET



# MARCO CIVIL INTERNET

**Art. 7º** O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)

**VII - não fornecimento a terceiros de seus dados pessoais**, inclusive registros de conexão, e de acesso a aplicações de internet, **salvo mediante consentimento livre, expresso e informado** ou nas hipóteses previstas em lei;

**VIII -** informações claras e completas **sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para finalidades que:

(...)

**IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais**, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

**X - exclusão definitiva dos dados pessoais** que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;



<https://acertech.com.br/wp-content/uploads/2018/11/marco-internet.png>

# PENALIDADES MARCO CIVIL INTERNET

**Art. 12.** Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

**II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;**

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

**Parágrafo único.** Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.



<https://www.projetodraft.com/verbete-draft-o-que-e-marco-civil-da-internet/>

# Carta Direitos Fundamentais UE

- Artigo 7º - Respeito pela vida privada e familiar
- Artigo 8º - Proteção de dados pessoais



<https://fra.europa.eu/pt/publication/2020/carta-dos-direitos-fundamentais-da-ue-utilizacao-e-valor-acrescentado-aos-estados>

# GDPR

GENERAL DATA PROTECTION REGULATION



Data Protection  
Officer (DPO)



Compliance



Violação de Dados



Dados Pessoais

# GDPR

- 04 anos de debate
- Aprovado em  
25/05/2016.
- Entrou em vigor em  
25/05/2018.
- Substituiu a Diretiva  
Europeia 95/46/EU



<https://lageeoliveira.adv.br/nosso-blog/gdpr-o-que-e/>

# PRINCÍPIOS GDPR

- Extranacionalidade
- Prestação de Contas
- Princípio da minimização
- Princípio do Armazenamento dos Dados Pessoais de interesse público, científico, histórico ou para fins estatísticos
- Transparência: dados pessoais direito subjetivo



<https://www.questionpro.com/blog/gdpr-survey/>

# PRINCÍPIOS GDPR

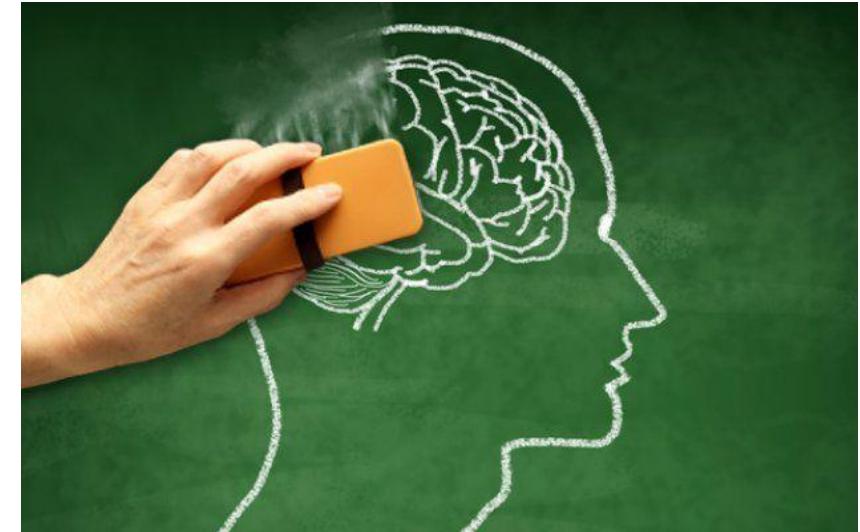
- Em 1995 a União Europeia não considerou os Estados Unidos como sendo um país com nível adequado no tocante à proteção de dados pessoais.
- No ano 2000, EUA e EU realizaram o **safe harbor** para garantir a transferência de dados entre eles.
- Em 2015 a Corte de Justiça Europeia anulou o **safe harbor** no julgamento do caso **Max Schrems vs. Data Protection Commissioner**, levando milhares de empresas a ficarem sem ter uma base legal para realizar as suas transações de dados.
- Essa situação perdurou até os EUA e a EU realizarem o **Privacy Shield** em 12/07/2016, com medidas que incluem esclarecimentos adicionais em coleta de dados em massa e a adoção do mecanismo de *Ombudsperson*, que é um representante da empresa que lidará com reclamações de usuários europeus sobre eventuais acessos por agências de inteligência americanas a seus dados pessoais.
- 2020 – Corte da União Europeia invalida o **Privacy Shield**.
- 10 de julho de 2023 – **Novo Marco Legal** entre EUA e UE. União Europeia reconhece que os EUA já possui nível para privacidade e proteção de dados.



<https://telesintese.com.br/uniao-europeia-e-eua-fecham-acordo-de-compartilhamento-de-dados-pessoais/>

# DIREITO AO ESQUECIMENTO

- Direito ao esquecimento
- Não existe no Brasil
- Deleção x Desindexação
- **CASO Google Espanha:** Em 2014, um cidadão espanhol ganhou o direito de ser desindexado pelo Google.

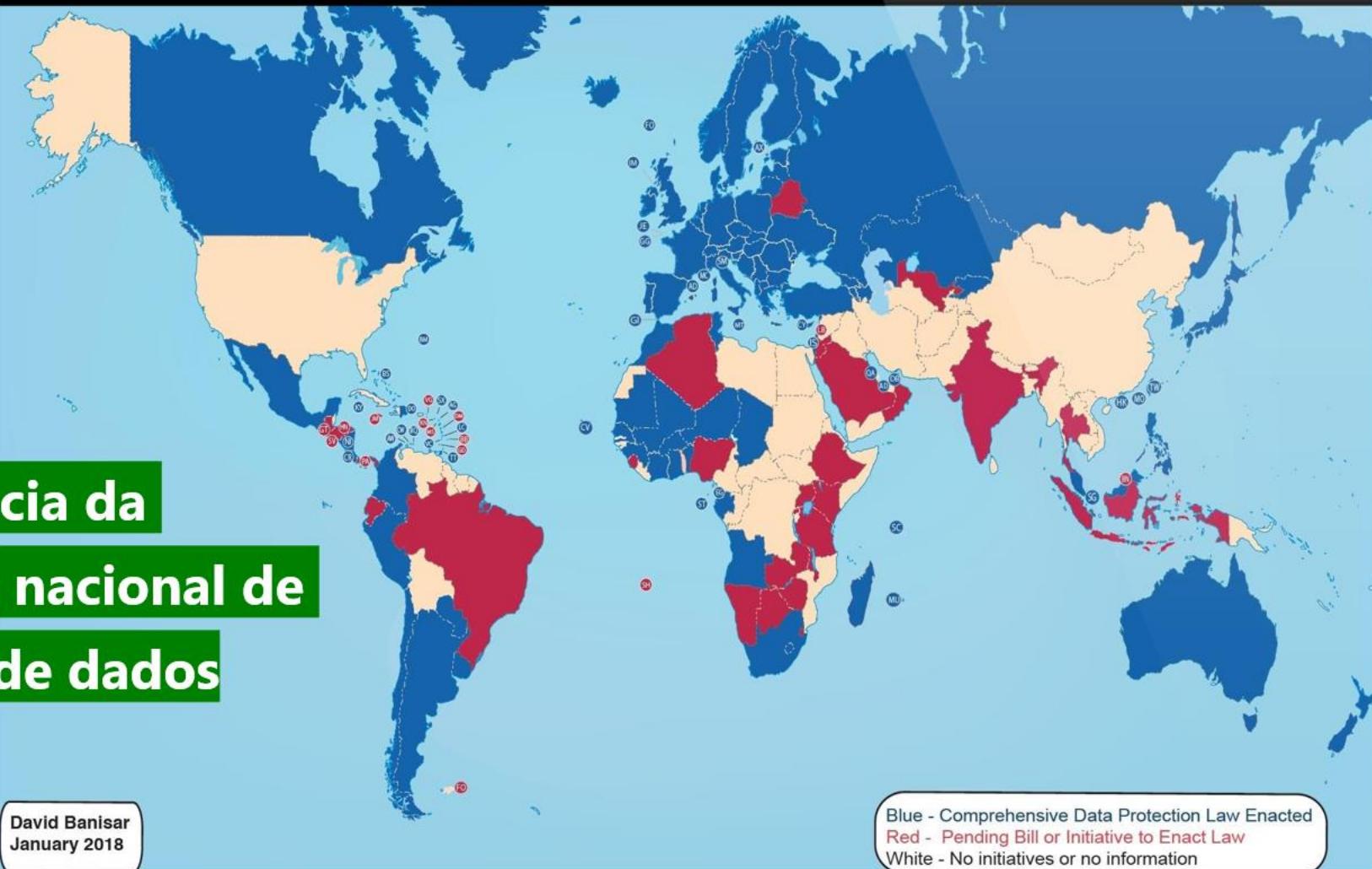


<https://www.jusbrasil.com.br/artigos/direito-ao-esquecimento/567496136>

# Abrangência da legislação nacional de proteção de dados

David Banisar  
January 2018

Blue - Comprehensive Data Protection Law Enacted  
Red - Pending Bill or Initiative to Enact Law  
White - No initiatives or no information





# PROTEÇÃO DE DADOS

## CHINA

# Proteção de dados

# EUA



# AMÉRICA LATINA

- CHILE:** Ley nº 19.628/1999.
- ARGENTINA:** 1994, alterada em 2000 e posteriormente em 2017.
- URUGUAI:** Ley nº 17.838/2004, revogada pela ley nº 18.331/2008.
- PARAGUAI:** Ley nº 1.682/2001
- MÉXICO:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicada no Diário Oficial em 05/07/2010).
- PERU:** LEI DE 2011



<https://brasilescola.uol.com.br/geografia/america-latina.htm>



# Cambridge

A N A L Y T I C A

# LGPD

LEI GERAL DE PROTEÇÃO DE  
DADOS



- Lei 13.709 de 14 de agosto de 2018
- Entrou em vigor em setembro de 2020.
- Sanções aplicadas a partir de agosto de 2021.

# Exceções LGPD

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

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais;



<https://mundoeducacao.uol.com.br/gramatica/excecao-ou-excessao.htm>



# Autodeterminação INFORMATACIONAL

Falta de **cultura de proteção** de dados





ITAÚ PRIVACIDADE 3 - Te amo tanto que até fiz uma camiseta com seus dados | 2021 | Comercial de TV  
Para sair do modo tela cheia, pressione Esc



Lalala.com.br



Arquivo Pessoal

## PP&D COMO DIFERENCIAL DE MERCADO

- Propaganda Itaú  
[https://youtu.be/FI55ZPL\\_NMo?si=ks-kMT2pE8OiKJXq](https://youtu.be/FI55ZPL_NMo?si=ks-kMT2pE8OiKJXq)
- Propaganda Apple  
[https://www.youtube.com/watch?v=wHh6Mzq\\_KdI](https://www.youtube.com/watch?v=wHh6Mzq_KdI)

# Lei Geral DE PROTEÇÃO DE DADOS

## ART. 5º PARA OS FINS DESTA LEI, CONSIDERA-SE:

- **DADO PESSOAL:** informação relacionada a pessoa natural **identificada ou identificável**;
- **DADO PESSOAL SENSÍVEL:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **TRATAMENTO:** **toda operação realizada com dados pessoais**, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;



# CONSTITUIÇÃO

DA REPÚBLICA

## EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022

**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

**X** - o direito a indenização pelo dano material ou moral decorrente de sua violação 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;

**LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.**



<https://livraria.senado.leg.br/constituicao-federal-livro>

# 10

## Princípios para o tratamento de dados de acordo com a LGPD

- 1 FINALIDADE**  
Apenas coletar dados pessoais para fins legítimos, informando com clareza o usuário a finalidade da coleta
- 2 ADEQUAÇÃO**  
Disponibilizar todas as informações sobre a coleta e uso de dados para o usuário de forma honesta
- 3 NECESSIDADE**  
Manter e utilizar apenas os dados essenciais, apagando-os quando deixarem de ser relevantes
- 4 LIVRE ACESSO**  
Ser capaz de apresentar ao usuário os dados e a forma como são processados ao ser requisitado
- 5 PRECISÃO**  
Manter os dados precisos a todo momento, deletando ou atualizando dados errados ou imprecisos
- 6 TRANSPARÊNCIA**  
O usuário deve ser informado de maneira clara e acessível sobre os riscos e direitos sobre seus dados
- 7 SEGURANÇA**  
Tomar medidas técnicas e administrativas para proteger os dados de danos, furtos ou perdas
- 8 PREVENÇÃO**  
Tomar medidas preventivas para a proteção dos dados, evitando danos aos titulares
- 9 NÃO DISCRIMINAÇÃO**  
Não utilizar os dados para nenhum fim discriminatório, ilícito ou abusivo, atendendo aos requisitos da lei
- 10 RESPONSABILIDADE**  
Comprovar a adoção em todos os procedimentos da empresa



# Tratamento

## DADOS PESSOAIS SENSÍVEIS

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

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

II - **sem fornecimento de consentimento do titular**, nas hipóteses em que for indispensável para:

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; ou

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



# Agentes

DE TRATAMENTO DE DADOS



É quem **toma as decisões referentes ao tratamento** de dados, ainda que não realize diretamente o tratamento em questão.

É quem **efetivamente trata os dados**, ainda que não tenha ingerência sobre seu tratamento.

# CONTROLADOR

- É parte responsável por garantir que os dados pessoais sejam processados de acordo com os regulamentos e normas.
- O Controlador que tem maior peso jurídico nas legislações de Privacidade e Proteção de Dados no mundo.
- Na maioria dos casos será a Parte com interface direta com o público que fornece informações e presta esclarecimentos.

Exemplo: um Escritório de Advocacia que usa o software de um terceiro para cadastrar os processos em sua Banca.



<https://www.doistercos.com.br/porta-dos-fundos-lanca-loja-de-camisetas-online/>

# CONTROLADOR - RESPONSABILIDADES

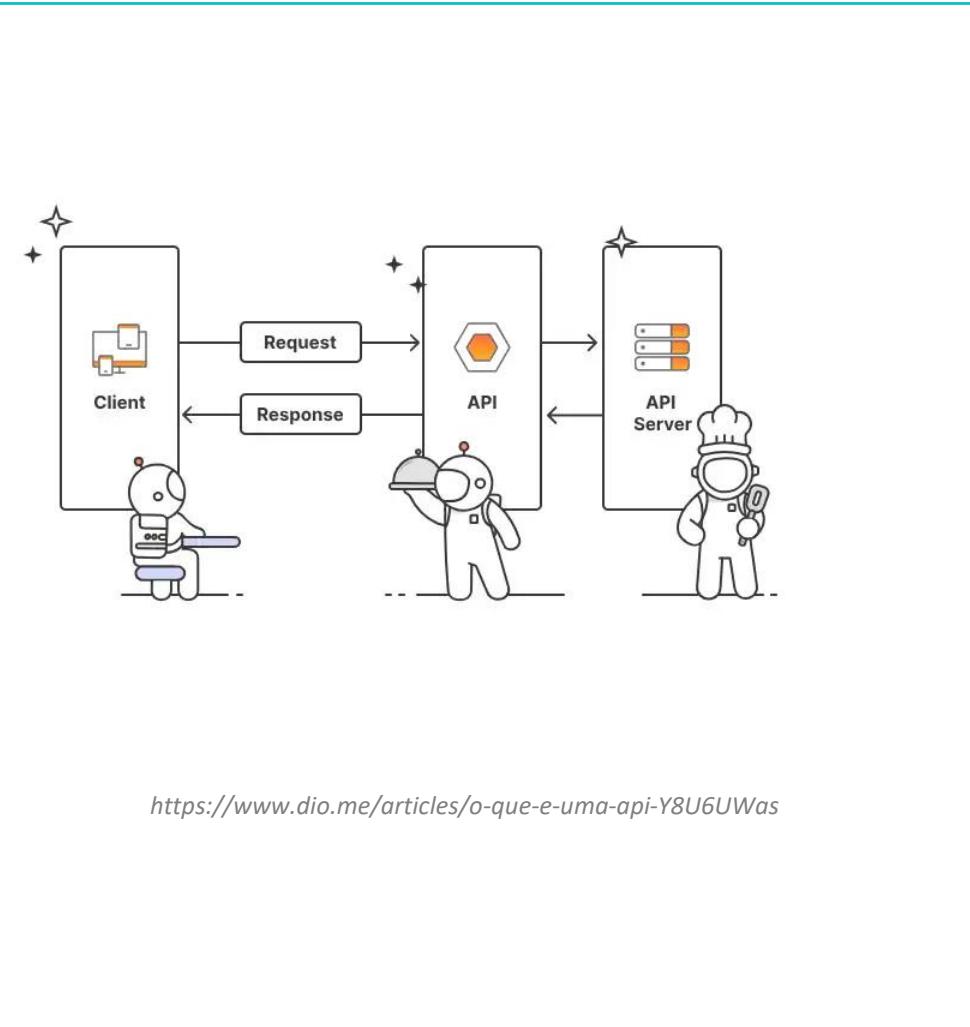
- Determina a finalidade das atividades de processamento.
- Designa o DPO
- Responsável pelos direitos dos Titulares
- Responsável por implementar as medidas técnicas e operacionais para garantir e demonstrar que age dentro da Lei e das normas técnicas
- Implementa as Políticas e os Documentos Jurídicos Regulatórios.
- Elabora o Relatório de Impacto de Dados
- Elabora o LIA
- Assegura que os Operadores e subcontratados estão em Compliance
- Notifica as violações de dados para as Autoridades Supervisoras.



<https://www.doistercos.com.br/porta-dos-fundos-lanca-loja-de-camisetas-online/>

# CONTROLADOR CONJUNTO

- Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento.
- O acordo pode designar um ponto de contacto para os titulares dos dados
- Fonte: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf)



<https://www.dio.me/articles/o-que-e-uma-api-Y8U6UWas>

# OPERADOR

- São entidades contratadas pelo controlador para execução de alguma função nos dados pessoais.
- Executam as atividades de processamento sob controle de um controlador.
- Responsáveis pela segurança do processamento de dados.
- Determinam os aspectos técnicos do processamento



<https://www.infranewstelcom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgd/>

# OUTRAS PARTES ENVOLVIDAS

- «**Subcontratante**», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.
  - «**Destinatário**», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro.
  - «**Terceiro**», não é o titular dos dados, o subcontratante que está autorizado a tratar os dados pessoais
- «**Representante**», uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27 da GDPR.



# DPO

DATA PROTECTION OFFICER

**ENCARREGADO DE DADOS PESSOAIS:** é o responsável por orientar colaboradores da empresa acerca das práticas relativas à proteção de dados, prestar esclarecimentos aos titulares de dados, receber comunicações da Autoridade Nacional e tomar as providências cabíveis.

## PESSOA FÍSICA OU JURÍDICA

Fonte: Privacy Point

# REGRAS SOBRE O ENCARREGADO

- Obrigatório para empresas e Entes Públicos. Ex. ANPD - [Thiago Guimaraes Moraes](#).
- Também é exigido para os Operadores que tratam dados em larga escala. [Ex. Mapa](#)
- Indicado e [IDENTIFICADO](#) no site do Controlador.
- Extremamente exposto ao Público e seus dados são difundidos para fornecedores, clientes e autoridades.
- Não é exigido para Startups e Terceiro Setor. <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>



# O fundamental papel do Encarregado

- Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
- O encarregado é o indivíduo ou EMPRESA responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD.



<https://www.impacta.com.br/blog/como-ser-um-data-protection-officer-dpo-entenda/>

# FUNÇÕES DO ENCARREGADO DE DADOS

1. Diagnóstico – *Data Inventory*
2. Construção das Políticas e documentos jurídicos regulatórios.
3. Comunicação interna (diretoria e stakeholders) e externa (clientes, fornecedores e Autoridades).
4. Mapeamento, Inventário Sistemas, Análise de Risco.
5. Coordenação de Resposta de Incidentes e **VIOLAÇÕES DE DADOS**.
6. Demais determinações do Controlador, *Ex. Gestão do Consentimento*.
7. **Sem glamour e muito trabalho.**



Fonte <https://www.apuliaonbike.com/camisa-do-zidane-real-madrid-k.html>

# RESPONSABILIDADE DO ENCARREGADO DE DAOS

- Não responde perante terceiros.  
Evite custos desnecessários como seguro D&O.
- Não é agente de tratamento.  
Exceção Filipinas e Indonésia
- Responde ao Controlador.  
Ex: falha grave na PDP ou previsões contratuais (DPA).

“LGPD. 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.”



<https://goadopt.io/blog/responsabilidades-de-um-encarregado-de-dados/>

# ENCARREGADO DE DADOS - CBO

- Planejam processos administrativos, financeiros, de Compliance, de riscos e de proteção de dados pessoais e privacidade. Gerenciam pessoas, rotinas administrativas e financeiras. Administram riscos, recursos materiais, serviços terceirizados e canal de denúncia.
- Participam da implementação do programa de compliance e/ou de governança em privacidade. Monitoram e avaliam o cumprimento das políticas do programa, normativas, código de ética, procedimentos internos e parceiros de negócios.
- Participam da identificação de situações de riscos e propõem ações para mitigação dos mesmos. Prestam atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais.



- Fonte: <http://www.mtecbo.gov.br/cbosite/pages/pesquisas/BuscaPorTituloResultado.jsf>

# DPO EXERCENDO OUTRAS FUNÇÕES

- Pode executar outras tarefas, desde que não haja **CONFLITO DE INTERESSES.**
- Parecer do grupo de trabalho do art. 29 GDPR do Conselho Europeu de Proteção de Dados.
- Posições conflitantes:
- CEO, CTO, CIO, COO, CFO, Diretor de Marketing, Diretor de Recursos Humanos, Advogado



The screenshot shows the EDPB website with the logo 'edpb European Data Protection Board'. A blue banner at the top right says 'SOBRE O CEPD ▾'. Below is a large image of two people walking on a path made of binary code. At the bottom, a blue bar contains the text 'Home > About EDPB > Legado: Grupo de Trabalho do Artigo 29.º'.

Legado: Grupo de Trabalho do Artigo 29.º

- Fonte [https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party\\_pt](https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_pt)

# VANTAGENS DPO TERCEIRIZADO

- Menor custo do que um DPO interno
- Maior experiência por atuar em várias empresas e entes públicos
- Maior especialização.
- Acionado a quando necessário.
- Facilita a independência por ser terceirizado.
- Sempre atualizado com as tecnologias recentes.



■ Fonte <https://www.rgtec.com.br/lgpd-1/dpo-as-a-service>

# O QUE AJUDA A VIDA DO DPO

1. Difundir a cultura de privacidade e proteção de dados.
2. Utilização de sistemas que automatizem a gestão do consentimento e emissão de relatórios, políticas e outros documentos de forma ágil.
3. Bom salário e autonomia, pois pode confrontar com a Alta Diretoria.
4. Ter uma equipe, *pois sozinho....*

<https://privacypoint.com.br/dist/index.php>

<https://www.dadoslegais.com.br/>

<https://www.onetrust.com/>



# CERTIFICAÇÃO DPO

EXIN

PDPE



ISFS



PDPF

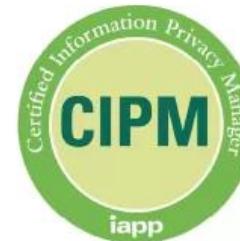
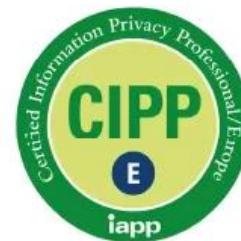


PDPP



<https://www.exin.com/pt-br/>

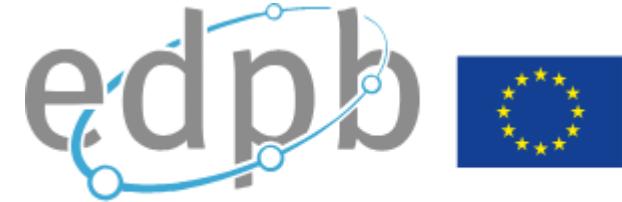
IAPP



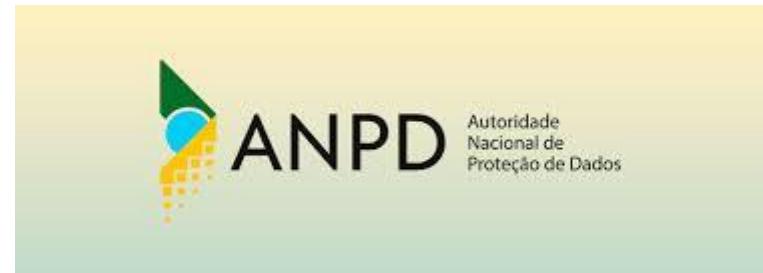
<https://iapp.org/resources/article/simple-data-protection-policy-template-2/>

# MATERIAIS GRATUITOS PARA O DPO

- Guidelines on Data Protection Officers
  - <https://ec.europa.eu/newsroom/article29/items/612048>
- Guias e Modelos ANPD
  - <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>
- ICO DOCUMENTATION
  - <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/documentation/>



European Data Protection Board



Information Commissioner's Office

# QUANTO VALE O SHOW? - SALÁRIO DPO/ENCARREGADO



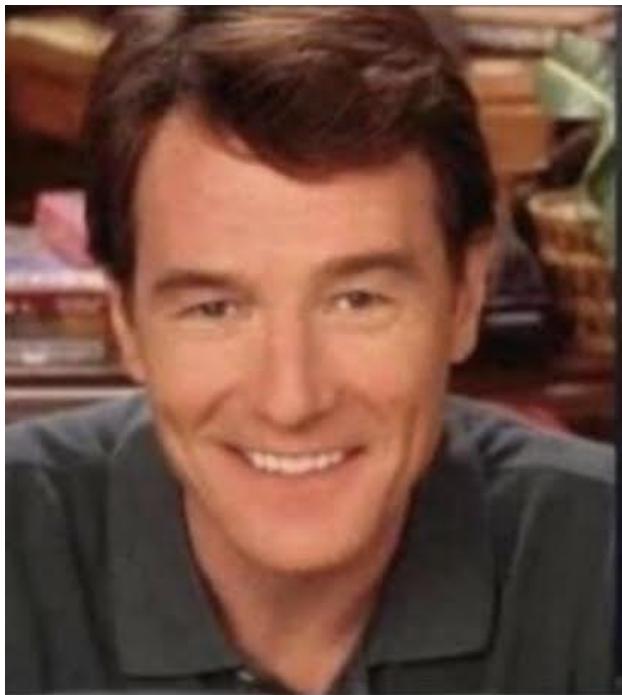
<https://www.impacta.com.br/blog/como-ser-um-data-protection-officer-dpo-entenda/>



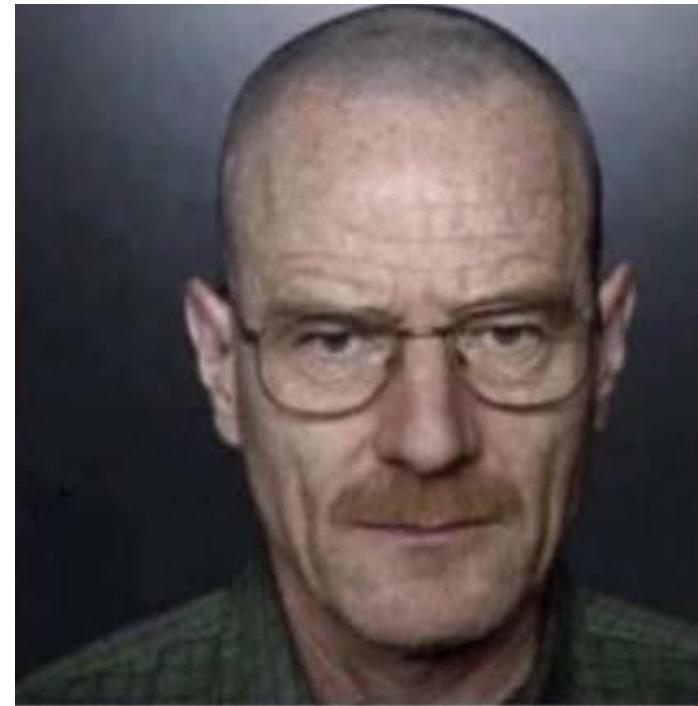
<https://br.pinterest.com/sergiotna/vetor-profiss%C3%B5es/>

# EXPEXTATIVA X REALIDADE

INÍCIO



UM ANO DEPOIS...



Ator Bryan Cranston

# Canal de Comunicação

## COM O TITULAR

**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:

- I. confirmação da existência de tratamento;
- II. acesso aos dados;
- III. correção de dados incompletos, inexatos ou desatualizados;
- IV. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- V. 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**;
- VI. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX. revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

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

- I. em formato simplificado, imediatamente; ou
- II. 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; ou
- II. sob forma impressa.

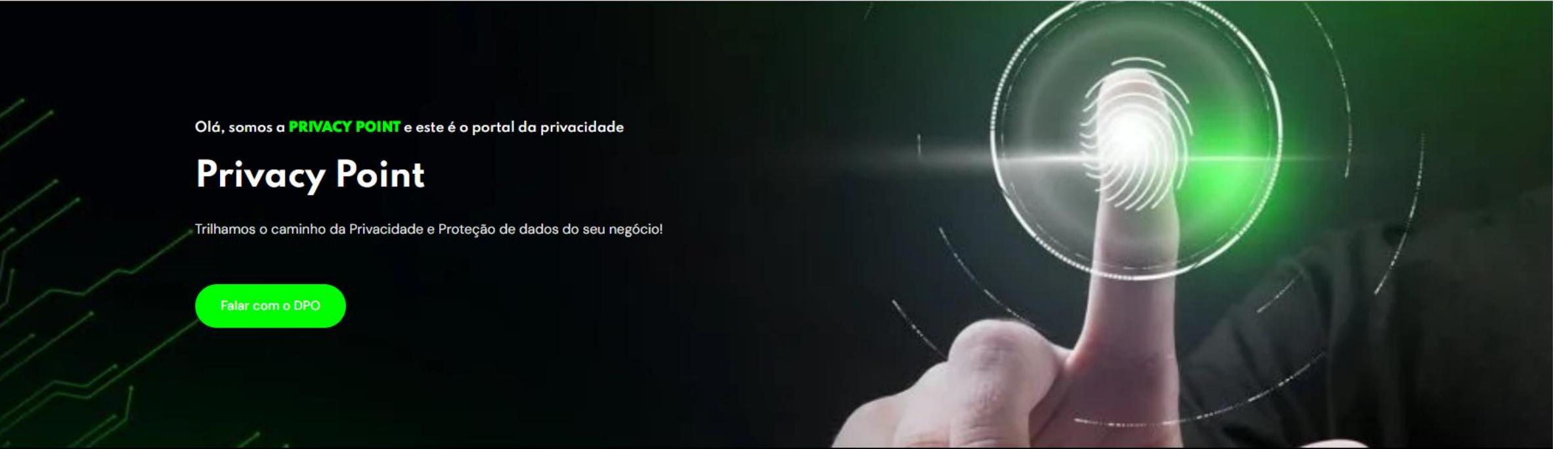
**§ 3º** Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

**§ 4º** **A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.**

# Canal de Comunicação

COM O TITULAR





Olá, somos a **PRIVACY POINT** e este é o portal da privacidade

# Privacy Point

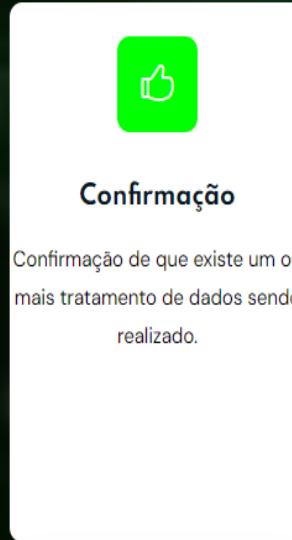
Trilhamos o caminho da Privacidade e Proteção de dados do seu negócio!

Falar com o DPO

Quais os seus direitos como

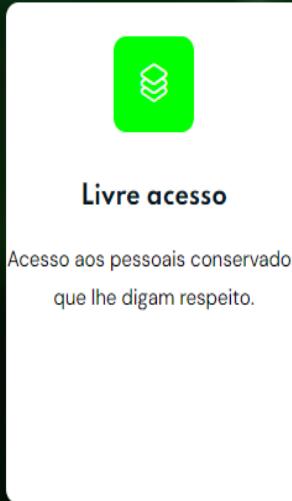
## TITULAR DOS DADOS

De acordo com o art.18 da LGPD, 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.



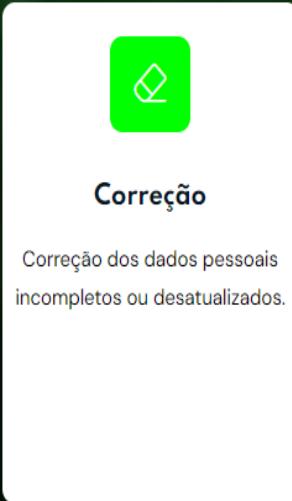
### Confirmação

Confirmação de que existe um ou mais tratamento de dados sendo realizado.



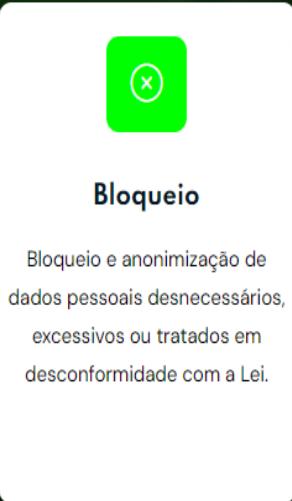
### Livre acesso

Acesso aos pessoais conservados que lhe digam respeito.



### Correção

Correção dos dados pessoais incompletos ou desatualizados.



### Bloqueio

Bloqueio e anonimização de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a Lei.



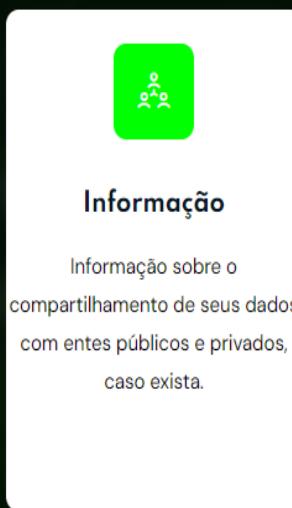
### Portabilidade

Portabilidade de dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial.



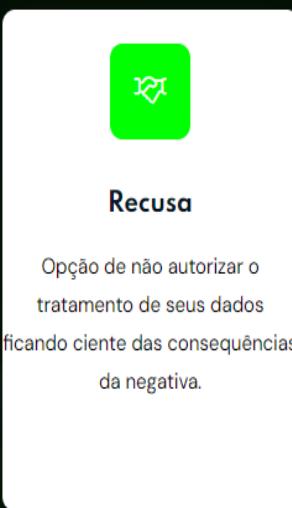
### Eliminação

Eliminação definitiva dos dados pessoais tratados (exceto quando o tratamento é legal, mesmo que com o consentimento do titular).



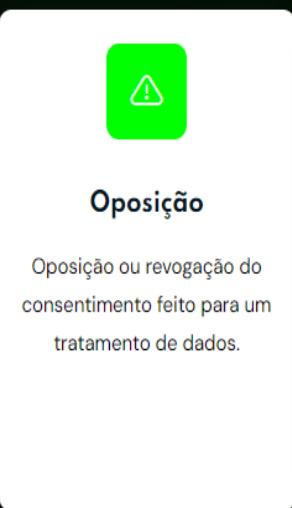
### Informação

Informação sobre o compartilhamento de seus dados com entes públicos e privados, caso exista.



### Recusa

Opção de não autorizar o tratamento de seus dados ficando ciente das consequências da negativa.



### Oposição

Oposição ou revogação do consentimento feito para um tratamento de dados.



### Reclamação

Reclamação contra o controlador dos dados junto à Autoridade Nacional (consentimento do titular).



# 1

## FINALIDADE

Apenas coletar dados pessoais para fins legítimos, informando com clareza ao usuário a finalidade da coleta.

# 2

## ADEQUAÇÃO

Disponibilizar todas as informações sobre a coleta e uso de dados para o usuário de forma honesta.

# 3

## NECESSIDADE

Manter e utilizar apenas os dados essenciais, apagando-os quando deixarem de ser relevantes.

# 4

## LIVRE ACESSO

Ser capaz de apresentar ao usuário os dados e a forma como são processados ao ser requisitado.

# 5

## PRECISÃO

Manter os dados precisos a todo momento, deletando ou atualizando dados errados ou imprecisos.

# 6

## TRANSPARÊNCIA

O usuário deve ser informado de maneira clara e acessível sobre os riscos e direitos sobre seus dados.

# 7

## SEGURANÇA

Tomar medidas técnicas e administrativas para proteger os dados de danos, furtos ou

# 8

## PREVENÇÃO

Tomar medidas preventivas para a proteção dos dados, evitando danos aos titulares.

# 9

## NÃO DISCRIMINAÇÃO

Não utilizar os dados para nenhum fim discriminatório, ilícito ou abusivo,

# 10

## RESPONSABILIDADE

Bloqueio e anonimização de dados pessoais desnecessários, excessivos ou

# 10 Princípios para Tratamento de Dados de acordo com a LGPD

## FALE COM O DPO



Siga a Privacy Point nas redes sociais:



Informe seu nome \*

Informe um e-mail para contato \*

Informe um telefone para contato \*

Informe sua solicitação \*

ENVIAR MENSAGEM



# Documentos

## E POLÍTICAS



**INVENTÁRIO**  
de dados



**POLÍTICA DE SEGURANÇA**  
da informação



**MAPEAMENTO**  
de dados



**CICLO DE VIDA**  
dos dados pessoais



**POLÍTICA**  
de privacidade



**MATRIZ**  
de risco



# Transferência INTERNACIONAL DE DADOS

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

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- A. cláusulas contratuais específicas para determinada transferência;
- B. cláusulas-padrão contratuais;
- C. normas corporativas globais;
- D. selos, certificados e códigos de conduta regularmente emitidos;

**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:

(...).

**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.

# BCR – Binding Corporate Rules

## REGULAMENTO EMPRESARIAL

Um grupo de empresas, ou um grupo de empresas envolvidas numa atividade econômica conjunta, deve poder utilizar as regras empresariais vinculantes aprovadas para as suas transferências internacionais da União para organizações pertencentes ao mesmo grupo de empresas ou grupo de empresas uma atividade econômica conjunta, desde que tais regras corporativas incluam todos os princípios essenciais e direitos aplicáveis para garantir as salvaguardas apropriadas para transferências ou categorias de transferências de dados pessoais.



Código de Conduta  
atualizado com a  
LGPD



Políticas de Privacidade  
e Segurança da  
Informação



Depende de  
chancela da  
ANPD





# Cláusulas Contratuais

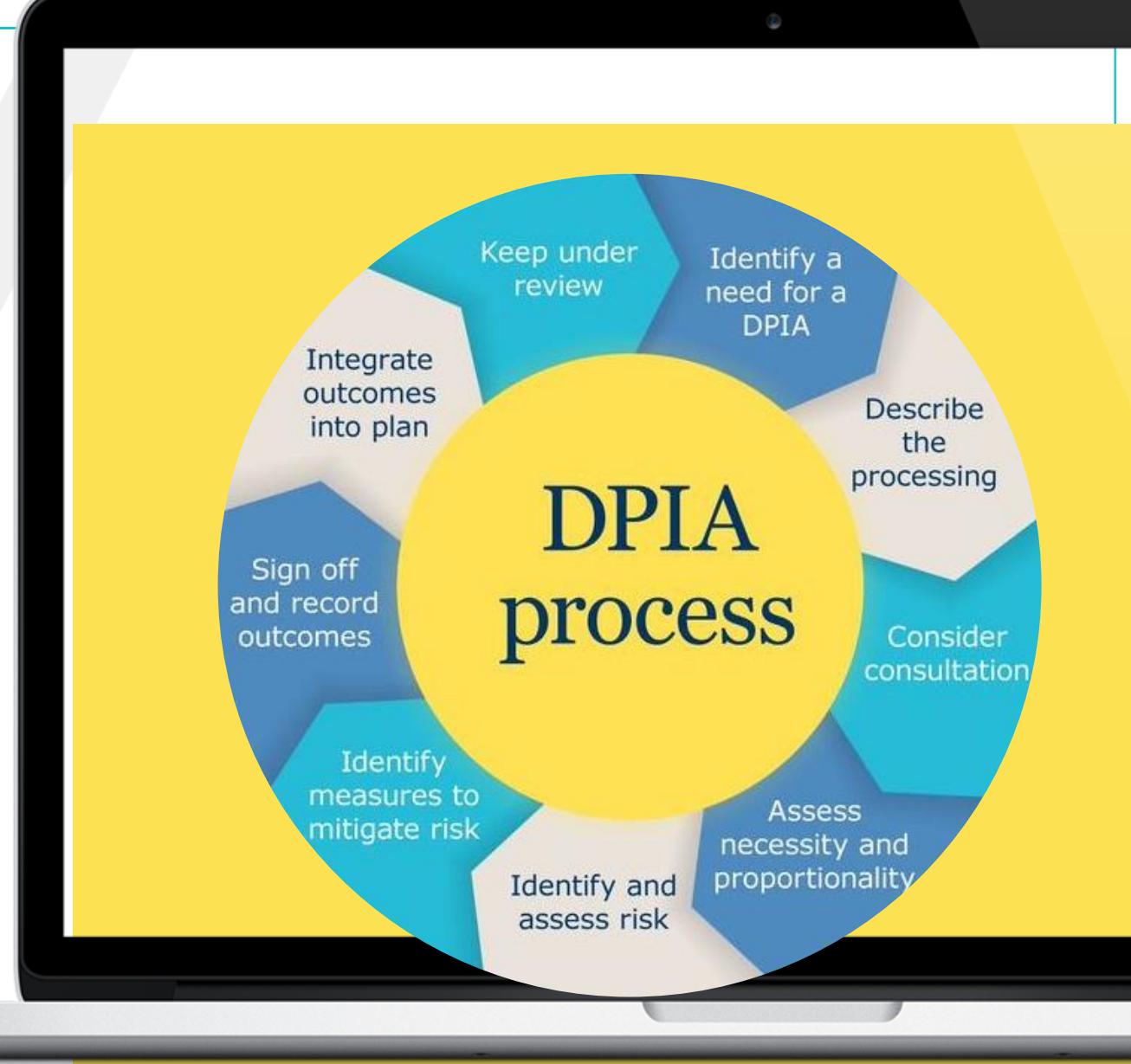
## PADRONIZADAS

A Autoridade Supervisora pode adotar cláusulas contratuais-padrão para o contrato vinculante entre o controlador e o processador e, se apropriado (por exemplo, com autorização prévia por escrito do controlador), entre o **CONTROLADOR** e o **OPERADOR**.

# Relatório de IMPACTO DE DADOS

**Art. 38.** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

**Parágrafo único.** Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.



# LGPD

## P E N A L I D A D E S

- 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 (...)
- VII. suspensão atividade empresária
- VIII. proibição da atividade empresária



# Dosimetria

## DA PENAL

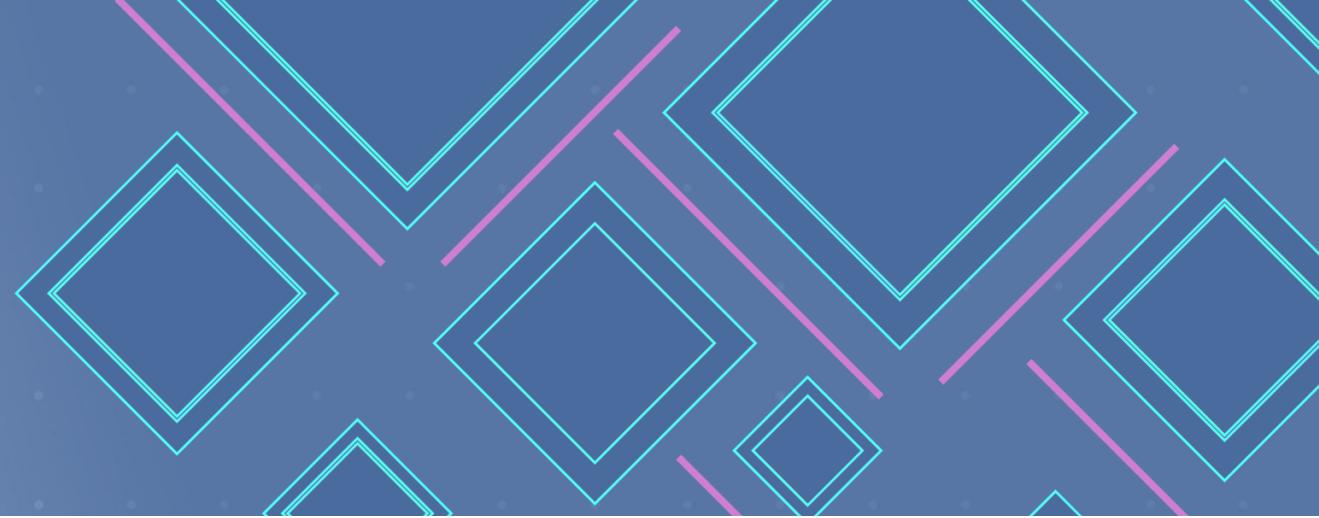


§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- 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; e
- XI. a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

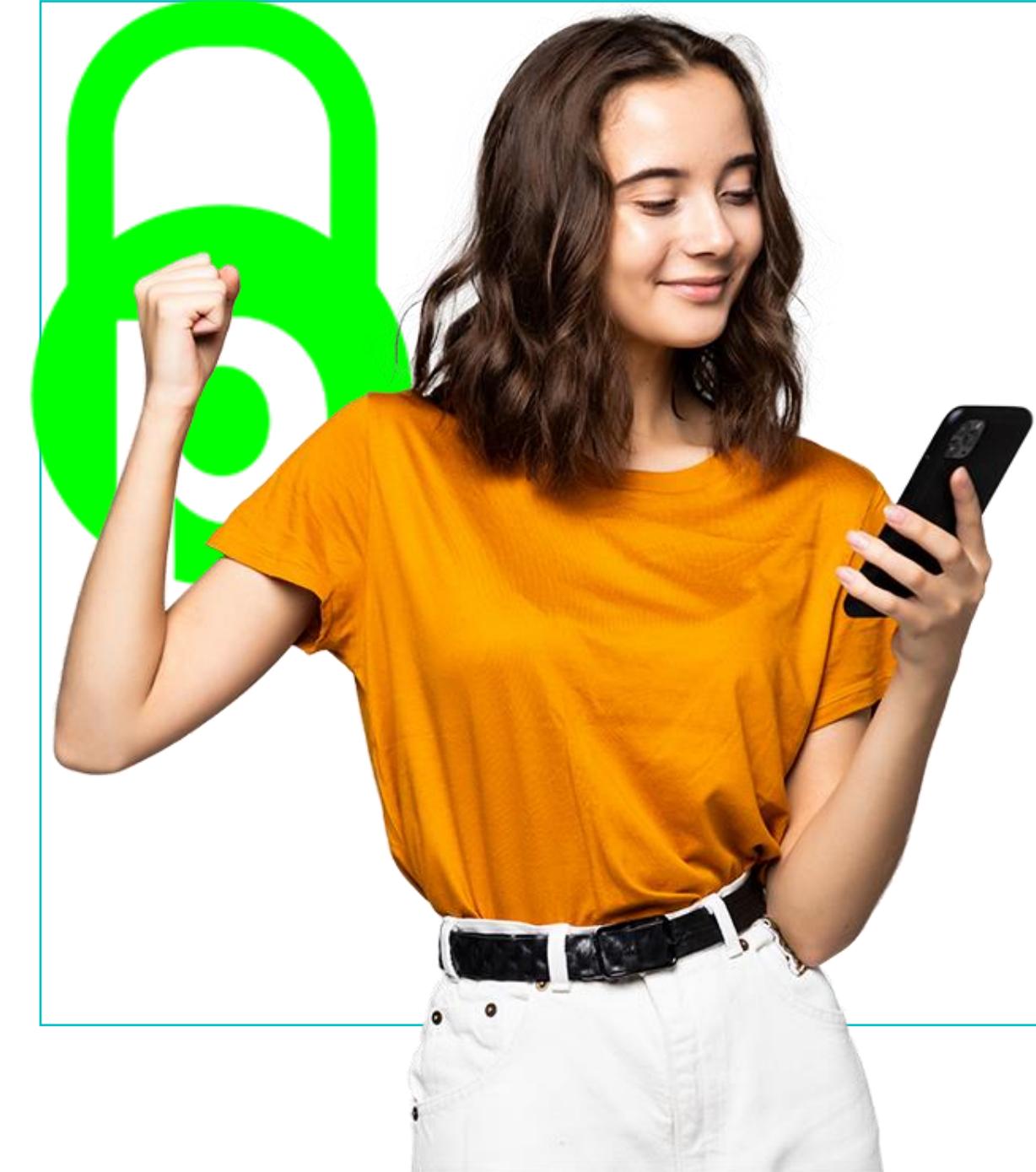


PUC Minas



# AUTORIDADES SUPERVISORAS





# ANPD

AUTORIDADE NACIONAL

DE PROTEÇÃO DE DADOS

Órgão em atividade.

Penalidades aplicadas desde

**1º de Agosto de 2021**

# FUNÇÃO ANPD

- Monitorar e fiscalizar a aplicação da LGPD.
- Aconselhar governos, empresas, e titulares sobre as medidas legislativas e administrativas.
- Chancelar cláusulas contratuais padrão.
- Aprovar e chancelar regras corporativas vinculantes/compulsórias.
- Manter registros internos das infrações da LGPD.



Fonte: <https://www.limajr.com.br/lgpd-regulamentacao-dados-um-olhar-sobre-a-dosimetria-e-aplicacao-de-sancoes-pela-anpd/>

# FUNÇÃO ANPD

## Poderes de **investigação**

Exemplo: realizar auditorias de proteção de dados, para notificar o responsável pelo tratamento ou o subcontratante de uma infração alegada.

## Poderes de **correção**

Exemplo: emitir advertências, multas.

Exemplo: realizar auditorias de proteção de dados, para notificar o responsável pelo tratamento ou o subcontratante de uma infração alegada.

## Poderes **consultivos e de autorização**

Exemplo: adotar cláusulas contratuais padrão, emitir e selos.



<https://www.vecteezy.com/vector-art/26530463-check-mark-seal-icon-vector>

# JULGAMENT STF – MP 954

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:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - 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

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

The screenshot shows a news article from the Migalhas website. The header of the page includes the logo 'migalhas' and the date 'quarta-feira, 6 de maio de 2020'. The main title of the article is 'Rosa Weber mantém suspensão de MP de compartilhamento de dados com IBGE'. Below the title, it says 'O julgamento de hoje contou com as sustentações orais e o voto da relatora.' and 'quinta-feira, 6 de maio de 2020'. The article discusses the judgment by the Federal Supreme Court (STF) against MP 954/20, which would have allowed the sharing of data from telecommunications companies with the IBGE. The court upheld a suspension order issued by Justice Rosa Weber. The article also mentions other actions proposed by the OAB, PSDB, PSOL, PSL, and PCdoB. On the right side of the page, there are sections for 'Informativo de hoje', 'apoiadores' (with a logo for ALOPESMUNIZ), 'fomentadores' (with a logo for IASP), and 'patrocínio'.

Fonte: <https://www.migalhas.com.br/>

# PRINCÍPIO DA ESPECIALIDADE - ANPD

Art. 55 J - XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

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.



Fonte <https://www.portaldaprivacidade.com.br/anpd-divulga-primeiro-balanco-das-suas-atividades/>

# SANÇÕES APLICADAS - ANPD

- Multa de pouco mais de 14k para um pequeno telemarketing.
- Exposição de dados cadastrais e de saúde. Não apresentou ROPA ou RIPD.
  - Advertência.
- Vazamento de dados cadastrais, de saúde e financeiros
  - “Publicização da infração através de comunicado na primeira página do site da instituição, bem como por meio de envio de mensagem para todos os usuários de seu aplicativo. Tanto o comunicado do site como o aviso no aplicativo devem ficar disponíveis por 60 dias.”



Fonte <https://putsnem.blogspot.com/2017/03/chato-bobo-feio.html>

# POSTURA - ANPD



Dirección Nacional de Protección  
de Datos Personales

<https://www.dataprotected.com.co/faq-proteccion-datos>



Fonte <https://ico.org.uk/>

# PRINCÍPIO DA COOPERAÇÃO - GDPR



<https://training.indegu.co.uk/shop/business/introduction-to-gdpr/>



<https://conexaoaduanas.com.br/entenda-sobre-o-mercosul/>

# PAPEL EDUCATIVO - ANPD

- Excelente papel educativo
- Diretrizes para todos praticarem a LGPD
- <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>
- Regulamento sobre as sanções e dosimetria das penas
- <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria>
- Regulamentos e Resoluções de fácil acesso
- <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>



<https://stock.adobe.com/es/search/images?k=bravo>



PUC Minas

# HIPÓTESES DE TRATAMENTO

# CONSENTIMENTO

- art. 5º, I, LGPD - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- Pode ser revogado a qualquer tempo, art. 8º, V, LGPD
- Segundo Renato Leite e Bruno Bioni, trata-se da **carta coringa** da LGPD



<https://br.pinterest.com/pin/278871401896034820/>

# Cumprimento de obrigação legal

- Base legal que autoriza o tratamento dos dados dos titulares sem que aja consentimento para cumprimento de determinações legais.
- Exemplo: encaminhamento dos dados do funcionário à CEF para recolhimento do FGTS.



*Ministério do Trabalho - Brasil*

# EXECUÇÃO CONTRATO

- Base legal que autoriza o agente de tratamento a tratar o dado do titular sem o seu consentimento, porém deve estar adstrito exatamente ao objeto do contrato.
- Contrato de trabalho
- Currículo – contrato preliminar
- Exemplo: Para emissão da nota fiscal referente a uma compra é necessário apenas o nome, CPF e endereço. É dispensável por exemplo a faixa salarial



<https://www.jusbrasil.com.br/artigos/tipos-de-contratos/833176031>

# Exercício regular do direito em processo judicial

- Base legal que autoriza o tratamento de dados tanto para propositura das ações judiciais quanto na prevenção de futuras ações.
- Deve-se observar o prazo prescricional da respectiva demanda
- Exemplo: arquivar os dados do ex-funcionário pelo prazo de dois anos – CLT – 30 ANOS - INSS



<https://www.migalhas.com.br/depeso/270315/vale-a-pena-insistir-no-processo-judicial>

# PROTEÇÃO DA VIDA

ART. 7º, VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;

- Somente em casos de URGÊNCIA E EMERGÊNCIA
- Exemplo: Transfusão sangue hospital em caso de vida ou morte



<https://www.ufsm.br/cursos/graduacao/palmeira-das-missoes/enfermagem/eventos/feira-da-saude>

# TUTELA DA SAÚDE

ART. 7º, VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

- Exemplo: exames laboratoriais, prescrição médica, fiscalização dengue



<https://www.ufsm.br/cursos/graduacao/palmeira-das-missoes/enfermagem/eventos/feira-da-saude>

# PESQUISA



FONTE: IBGE

# POLÍTICAS PÚBLICAS

FONTE: GOVERNO FEDERAL



# PROTEÇÃO AO CRÉDITO

- JABOTICABA: Único País do mundo que tem essa base legal.
  - Lei do Cadastro Positivo
  - Open Finance
- 
- Exemplo: dados Serasa, conta bancária, fundos, cartão de crédito.



<https://consultacpfcnpjonline.com/familiares-negativados-podem-ser-registrados-no-cadastro-positivo-spcserasa/>

# LEGÍTIMO INTERESSE

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- I - apoio e promoção de atividades do controlador; e
- II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.



<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse>

# Legítimo

RESSE

## TESTE DOS QUATRO PASSOS

(LIA – Art. 37, caput, da LGPD)

**LEGITIMIDADE DO  
INTERESSE**  
(Art. 10, caput e  
inciso I da LGPD)

**NECESSIDADE**  
(10, §1º da LGPD)

**BALANCEAMENTO**  
(Art. 6º, I, 7º, IX e Art.  
10, II, da LGPD)

**SALVAGUARDA**  
(10, §2º e §3º da  
LGPD)

Finalidade  
Legítima

Minimização  
(menos intrusivo)

Legítima Expectativa  
(compatibilidade)

Transparência

Situação  
Concreta

Outras Bases Legais

Direitos e  
Liberdades  
Fundamentais

Mecanismos de  
Oposição (opt-out)

Adequação + Boa Fé  
(contexto)

Mitigação dos Riscos  
(e.g., anonimização)  
Outros Princípios PDP

# EXEMPLOS



<https://dataprivacy.com.br/>



# POLÍTICAS E DOCUMENTOS JURÍDICOS - REGULATÓRIOS



# Enquadramento do agente de tratamento de dados

CLIENTE É CONTROLADOR?  
CLIENTE É CONTROLADOR  
CONJUNTO?  
CLIENTE É OPERADOR?

E AÍ DPO?



# Treinamento da equipe



CERTIFICADOS

# CERTIFICADO



Certificamos que Denise França participou do treinamento

## **LGPD e Privacidade de Dados - Conceitos Básicos**

com duração de 1 hora, realizado pela PRIVACY POINT.

Belo Horizonte - MG, 12/06/2023

A handwritten signature in blue ink, appearing to read "d." followed by a surname.

Frederico Soares Ribeiro  
Especialista em inovação  
e privacidade

A handwritten signature in blue ink, appearing to read "L.F.S." followed by a surname.

Luiz Felipe Vieira de Siqueira  
Advogado Direito Digital



# Cartilha de Privacidade e Proteção de dados pessoais



FONTE PRIVACY POINT

priv<sup>acy</sup>  
point

# Cartilha para colaboradores

Belo Horizonte / MG

FONTE: PRIVACY POINT



FONTE: Privacy Point



# Políticas diversas



Política de Privacidade



Política de Segurança da Informação



Código de Ética



# Políticas

## De **PRIVACIDADE**



Aviso de Privacidade



Política de Privacidade Interna



<https://termly.io/resources/articles/privacy-notice-vs-privacy-policy/>

## Aviso de Privacidade

### 1. Sobre este Aviso de Privacidade

Este Aviso de Privacidade tem o objetivo de informar, de maneira objetiva e transparente, como o \*\*\*\*\* trata os dados pessoais dos pacientes, médicos, funcionários e prestadores de serviços. O \*\*\*\*\* é responsável pelo tratamento desses dados e está comprometido em proteger a privacidade e a segurança das informações.

### 2. Quais tipos de dados pessoais utilizamos?

Para o desempenho de nossas atividades, podemos tratar as seguintes categorias de dados pessoais:

- **Cadastrais e de identificação:** como nome, qualificação pessoal, endereço e informações identificadoras perante o cadastro de órgãos públicos (por exemplo, número de Cadastro de Pessoas Físicas - CPF).
- **Relacionados a comunicações eletrônicas:** como correio eletrônico (e-mail), endereço IP e informações sobre páginas acessadas.
- **Informações sobre interação de titular com agentes de tratamento:** quando fornecidas no conteúdo de petição de titular dirigida ao hospital.
- **Informações sobre denúncias:** como dados pessoais do denunciante nos canais oficiais do Hospital Socor S/A.

### 3. Por que e como tratamos seus dados pessoais?

Podemos tratar seus dados pessoais para o cumprimento das competências institucionais do \*\*\*\*\*\*, como as previstas na Lei Geral de Proteção de Dados Pessoais (LGPD). Isso inclui atividades como atendimento médico, gestão de recursos humanos, faturamento, execução de contratos com operadoras de planos de saúde e comunicação com pacientes e colaboradores.

Ao compartilharmos seus dados pessoais com operadores de dados, exigiremos que seus dados sejam tratados de acordo com nossas instruções, incluindo o armazenamento seguro, sua retenção apenas pelo período instruído e o não compartilhamento subsequente com outras organizações sem nossa prévia e expressa autorização.

### 4. Seus direitos de titular de dados pessoais

Como titular de dados pessoais, você tem direito a:

- Acessar seus dados pessoais.
- Corrigir dados incompletos, inexatos ou desatualizados.
- Solicitar a exclusão de dados desnecessários ou tratados em desconformidade com a lei.
- Obter informações sobre o compartilhamento de seus dados.
- Revogar o consentimento, quando aplicável.

### 5. Detalhes de contato

Em caso de dúvidas ou para exercer seus direitos, entre em contato com nosso Encarregado pelo Tratamento de Dados Pessoais:

Nome do Encarregado: [PRIVACY POINT CNPJ: \\*\\*\\*\\*\\*](#) E-mail: [dpo@privacypoint.com.br](mailto:dpo@privacypoint.com.br)

# POLÍTICA DE PRIVACIDADE INTERNA

## Categoria de Titular

## Finalidades do Tratamento

## Dados Tratados

## Exercício de direitos

- Beneficiários de Seguros intermediados pela SEGURADORA:**
- Colaboradores de empresas clientes da Empresa
  - Dependentes de colaboradores de empresas clientes da Seguradora

Prestar regularmente os serviços para os quais a Seguradora foi contratada, inclusive monitorar e apoiar beneficiários na utilização dos seguros

Manter contato com o titular, por meio de troca de e-mails, troca de cartões de visita, e do canal de atendimento ao consumidor

Viabilizar a realização de medidas de personalização da experiência dos consumidores/clientes, bem como eventuais campanhas de marketing e divulgação, além do uso de softwares e aplicativos para administração das atividades da Seguradora

Cumprir obrigações legais impostas à Seguradora, incluindo normas laborais, de segurança do trabalho e normas fiscais

Permitir o resguardo dos interesses da SKEMA BRASIL em situações como auditorias internas, operações de manutenção da segurança e eventuais processos judiciais, arbitrais ou administrativos

- **Dados pessoais:** Nome completo, CPF, data de nascimento, gênero, estado civil, nome da mãe, endereço, CNS, email, telefone, número de matrícula, data de admissão, cargo, dados vinculados ao seguro intermediado pela Exclusive.
- **Dados pessoais sensíveis:** Descritivos de utilização do plano (procedimentos realizados, estabelecimentos em que realizou), CID de afastamento, relatórios médicos e de exames

Nessas atividades, a SEGURADORA atua como operadora, ou seja, trata dados pessoais exclusivamente de acordo com as instruções das empresas clientes. Caso deseje exercer direitos previstos na LGPD, o titular deve entrar em contato diretamente com a empresa cliente da SEGURADORA, que atua como controladora dos dados pessoais e é responsável por responder às solicitações de titulares.



# POLÍTICA SEGURANÇA DA INFORMAÇÃO

<https://blog.almeidamatheus.me/post/politica-de-seguranca-da-informacao/>

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## Sumário

1. GLOSSÁRIO.....	4	5.23. REDES SOCIAIS, WHATSAPP E E-MAIL PESSOAIS .....	39
2. INTRODUÇÃO.....	6	5.24. JOGOS .....	40
3. OBJETIVOS.....	6	5.25. SOFTWARES .....	41
4. APLICAÇÃO.....	7	5.26. ACESSO FÍSICO AO CENTRO DE PROCESSAMENTO DE DADOS (CPD).....	41
5. CONDIÇÕES GERAIS.....	8	5.27. AUDITORIAS.....	42
5.1. PRINCÍPIOS .....	8	5.28. PRESTAÇÃO DE CONTAS - RESPONSABILIZAÇÃO .....	43
5.2. REQUISITOS.....	8	5.29. DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.....	44
5.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO.....	9	5.30. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO.....	44
5.4. RESPONSABILIDADES .....	10	5.31. DISPOSIÇÕES FINAIS .....	45
5.4.01. Usuários.....	10	5.32. CONTATOS IMPORTANTES.....	45
5.4.02. Responsáveis Hierárquicos .....	12		
5.4.03. Núcleo de Suporte a Informática (NSI).....	14		
5.5. RECURSOS COMPUTACIONAIS.....	18		
5.6. CONTROLE DE IDENTIFICAÇÃO (LOGIN E SENHA).....	18		
5.7. USO DE CREDENCIAIS PRIVILEGIADAS .....	19		
5.8. DISPOSITIVOS PESSOAIS .....	21		
5.9. TELA E MESAS LIMPAS.....	22		
5.10. MÍDIAS REMOVÍVEIS E DA PORTA USB.....	23		
5.11. DESCARTE DE MÍDIAS .....	23		
5.12. CLASSIFICAÇÃO DA INFORMAÇÃO.....	24		
5.12.01. Sigilo e Confidencialidade.....	26		
5.12.02. Comunicação Verbal.....	28		
5.13. PROTEÇÃO: ANTIVÍRUS .....	29		
5.14. E-MAIL CORPORATIVO .....	29		
5.15. A REDE DA SKEMA .....	32		
5.15.01. Direito de Uso .....	32		
5.15.02. Responsabilidades Individuais.....	32		
5.16. DISPOSITIVOS MÓVEIS .....	33		
5.17. HOME-OFFICE.....	34		
5.18. UTILIZAÇÃO DE IMPRESSORAS E OUTROS RECURSOS .....	35		
5.19. ADIÇÃO DE RECURSOS/EQUIPAMENTOS À REDE SKEMA.....	36		
5.20. ARMAZENAMENTO DE ARQUIVOS DE TRABALHO .....	37		
5.21. BACKUP DE ARQUIVOS .....	37		
5.22. UTILIZAÇÃO DA INTERNET.....	38		



# CÓDIGO DE CONDUTA

[https://www.nexusbr.com/pt\\_br/blog-inovacao-saneamento/entry/codigo-de-conduta](https://www.nexusbr.com/pt_br/blog-inovacao-saneamento/entry/codigo-de-conduta)

# CÓDIGO DE CONDUTA EXEMPLO

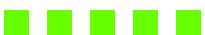
## SUMÁRIO

1.	INTRODUÇÃO .....	3
2.	DEFINIÇÕES.....	3
3.	DO RESPONSÁVEL PELO PROGRAMA DE INTEGRIDADE .....	4
3.1	Da coordenação do Programa de Integridade .....	4
3.2	Do Comitê de Ética .....	5
4.	CONTATO COM O AGENTE PÚBLICO.....	6
4.1	Anticorrupção.....	6
4.2	Conflito de interesse .....	7
5.	CONTATO COM OS PRESTADORES DE SERVIÇO .....	7
5.1	Do contrato de prestação de serviço de terceiros .....	7
5.2	Assédio .....	8
6.	CONTATO COM CONCORRENTES .....	8
6.1	Da preservação da concorrência .....	8
6.2	Das fusões e Aquisições .....	9
7.	DA CONDUTA ESPERADA DO COLABORADOR.....	9
8.	DOS DADOS PESSOAIS.....	10
8.1	Da confidencialidade .....	10
8.2	Política de acesso .....	10
9.	POLÍTICAS DE BRINDES E HOSPITALIDADE .....	10
9.1	Brindes e presentes .....	10
9.2	Hospitalidade .....	11
9.3	Doação .....	11
10.	DA LAVAGEM DE DINHEIRO .....	11
11.	DOS REGISTROS CONTÁBEIS .....	12
12.	COMUNICAÇÃO E TREINAMENTO.....	12
13.	CANAL DE DENÚNCIA .....	13
14.	DAS MEDIDAS DISCIPLINARES.....	13

# Termo de consentimento para tratamento de dados



Fonte: Privacy Point



# TERMO DE CONSENTIMENTO



Bem-vindo(a)! Obrigado por utilizar e fazer parte da PRIVACY POINT.

PRIVACY POINT, pessoa jurídica de direito privado, inscrita no CNPJ sob nº XXXXXXXXXX, com estabelecimento na \*\*\*ENDERECO\*\*\*.

Quando você entra em contato conosco e utiliza o nosso site ou nossos serviços, você nos confia dados pessoais e informações e, por isso, o nosso compromisso é manter essa confiança.

A PRIVACY POINT é comprometida a tratar os seus dados pessoais dentro da cultura de privacidade e proteção de dados em atenção à LGPD – Lei 13.709/18, que é um direito fundamental de qualquer cidadão.

Para isso, temos o TERMO DE CONSENTIMENTO abaixo, o qual explica como seus dados são tratados e para quais finalidades, conforme a LGPD.

## TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

### 1 – Tratamento de Dados Pessoais

A PRIVACY POINT é classificada como CONTROLADORA de dados e possui o Manual do Controlador.

Você, Titular dos Dados Pessoais, autoriza de modo inequívoco o uso de seus dados pessoais à Operadora, tendo como finalidade o tratamento de dados conforme disposto no item três deste instrumento. Serão fornecidos à Operadora: a) Nome completo; b) e-mail; c) número da Carteira de Identidade (RG); d) número do Cadastro de Pessoas Físicas (CPF); e) endereço completo; f) números de telefone e WhatsApp e g) dados biométricos para segurança dos alunos e dos estabelecimentos da PRIVACY POINT.

### 2 – Consentimento sobre o Tratamento de Dados Pessoais Sensíveis

O(a) Titular dos dados pessoais autoriza de modo inequívoco o tratamento de seus dados pessoais sensíveis pela Operadora, sendo disponibilizado a esta última: os dados referentes à saúde do(a) Titular, tal como a avaliação psicológica elaborada pelo sistema da PRIVACY POINT, o qual é registrado pelo Conselho Regional de Psicologia e protegido pelo segredo comercial.

### 3 - Finalidade do Tratamento dos Dados

A Operadora fica autorizada a tratar os dados pessoais e dados pessoais sensíveis listados neste termo para as seguintes finalidades:

- Permitir que a Operadora identifique e entre em contato com o Titular dos Dados, em razão da elaboração da avaliação psicológica realizada.

- Para cumprimento, pela Operadora, de obrigações legais impostas por órgãos de fiscalização no que concerne à avaliação psicológica realizada.
- Quando necessário para a executar um contrato, no qual seja parte o Titular dos Dados;
- A pedido do Titular dos Dados;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para a proteção da vida ou da incolumidade física do Titular dos Dados;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais habilitados, conforme determinações do Conselho Regional de Psicologia;
- Quando necessário para atender aos interesses legítimos do Controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção especial dos dados pessoais;

### 4 - Responsabilidade pela Segurança de Dados

A Controladora se responsabiliza por manter medidas de segurança, dentro das boas práticas e governança por via de técnicas suficientes a proteger os dados pessoais do Titular dos Dados. Caso haja qualquer incidente de segurança dos dados, a Controladora irá informar tanto ao Titular dos Dados quanto à Autoridade Nacional de Proteção de Dados (ANPD), no prazo de vinte e quatro horas após a ciência do fato.

### 5 - Término do Tratamento de Dados

À Operadora, fica autorizada para tratar os dados pessoais do Titular durante todo o período contratualmente firmado com o Controlador, para as finalidades relacionadas nesse termo e ainda após o término da contratação, para cumprimento de obrigação legal ou imposições realizadas por órgãos de controle estatal, nos termos do artigo 16 da Lei Geral de Proteção de Dados.

### 6 – Consentimento de Política de Privacidade e Proteção de Dados Pessoais

O Titular declara ter lido e estar de pleno acordo com a Política de Privacidade da SKEMA, disponível no site [www.PRIVACYPOINT.com.br](http://www.PRIVACYPOINT.com.br), estando ciente de que esta Política de Privacidade integra o presente Termo de Consentimento para todos os fins de direito.



# TERMO DE CONSENTIMENTO

## CRIANÇAS E ADOLESCENTES

### TERMO DE CONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E/OU ADOLESCENTES

Nome do Titular (Criança ou Adolescente):

Data de Nascimento: .....

CPF: .....

Dados de um dos Pais ou do Representante Legal:

Nome: .....

CPF: .....

Considerando que:

(i) Em conformidade com a Lei nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse;

(ii) De acordo com o art. 14, parágrafo 1º da LGPD, 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;

(iii) A PRIVACY POINT trata dados de crianças e adolescentes que figuram como alunos **com a finalidade de serviços acadêmicos e ofertas de cursos**;

(iv) A PRIVACY POINT preza pelo correto tratamento de dados pessoais e integral respeito da legislação sobre proteção de dados pessoais em vigor.

O signatário deste Termo de Consentimento para Tratamento de Dados Pessoais de Crianças e/ou Adolescentes ("Termo") consente com o tratamento de dados pessoais do Titular pela Exclusive Seguros nas seguintes condições:

#### 1. Da condição de pais ou representante legal do Titular

1.1 Ao firmar este Termo, os Pais ou Responsáveis declaram serem detentor de todos os poderes legais necessários à representação do titular.

#### 2. Do Tratamento de Dados Pessoais

2.1 Os dados pessoais serão tratados pela Exclusive Seguros para finalidades específicas, da forma e pela duração abaixo indicadas.

Finalidade	Dados Pessoais	Duração
Coleta e transferência de dados pessoais do Titular para a PRIVACY POINT, a qual presta serviços acadêmicos.	Nome e-mail CPF ****	Os dados pessoais serão armazenados pela PRIVACY POINT pelo prazo determinado em seu Ciclo de Dados.
Coleta e transferência de dados pessoais do Titular PRIVACY POINT.	Nome e-mail CPF	Os dados pessoais serão armazenados pela PRIVACY POINT pelo prazo determinado em seu Ciclo de Dados.

2.2 Mediante solicitação do Ministério da Educação, Secretarias de Educação e outros entes públicos, a PRIVACY POINT poderá auxiliar na coleta de dados pessoais adicionais.

2.3 O Titular poderá não consentir com os tratamentos de dados pessoais descritos nesta cláusula ou consentir com o tratamento de dados pessoais para apenas para uma das finalidades descritas. A consequência da negativa acarretará a impossibilidade de prestação de serviços acadêmicos.

2.4 O consentimento outorgado por meio deste Termo poderá ser revogado a qualquer momento, mediante solicitação encaminhada através do Canal de Proteção de Dados. Neste caso, a PRIVACY POINT cessará a transferência de dados pessoais às Operadoras, o que acarretará a interrupção da prestação dos serviços e impedirá a utilização do benefício.

2.5 Ainda que revogado o consentimento, a PRIVACY POINT poderá continuar tratando os dados pessoais na medida em que a lei permitir, como por exemplo, para exercer seus direitos em eventual processo judicial, administrativo ou arbitral ou para cumprimento de uma obrigação legal ou regulatória. Uma vez atingida a finalidade para a qual os dados pessoais são tratados, a PRIVACY POINT cessará o tratamento.

2.6 Para conhecer mais sobre como a PRIVACY POINT trata dados pessoais, visite nossa Política de Privacidade disponível em \*\*\*\*\*. O Titular ou seu representante poderão entrar em contato conosco e/ou exercer seus direitos previstos no art. 18 da lei 13.709/2018 através do e-mail [dpo@privacypoint.com.br](mailto:dpo@privacypoint.com.br).

Dante de todo o exposto, o representante do Titular **CONSENTE com o tratamento dos dados do menor de idade para as finalidades abaixo sinalizadas:**

Tratamento de dados pessoais para prestação de serviços acadêmicos e ofertas de cursos;

Local, data:

Assinatura de um dos pais ou  
Representante Legal

# Contratos reformulados de Proteção de Dados

-  Anexo de Privacidade e Proteção de Dados
-  Aditivo ao contrato de trabalho
-  Aditivo de contratos (Geral)
-  Contrato de trabalho



FONTE: Privacy Point

# ADITIVO PRIVACIDADE E PROTEÇÃO DE DADOS

## ADITIVO CONTRATUAL

### TERMOS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

1. CLÁUSULA PRIMEIRA – DAS DEFINIÇÕES

2. CLÁUSULA SEGUNDA – DAS RESPONSABILIDADES

3. CLÁUSULA TERCEIRA – DO TRATAMENTO DE DADOS PESSOAIS

4. CLÁUSULA QUARTA – COMPARTILHAMENTO COM TERCEIROS

4.1 DA SUBCONTRATAÇÃO

5. CLÁUSULA QUINTA - TRANSFERÊNCIAS INTERNACIONAIS

6. CLÁUSULA SEXTA – DA AUDITORIA

7. CLÁUSULA SÉTIMA – DA GESTÃO DE INCIDENTES

8. CLÁUSULA OITAVA – DA RESPONSABILIDADE E INDENIZAÇÃO

9. CLÁUSULA NONA – DA ASSISTÊNCIA

10. CLÁUSULA DÉCIMA - DO TÉRMINO DO TRATAMENTO DE DADOS

11. CLÁUSULA PRIMEIRA – DAS DISPOSIÇÕES DIVERSAS E FORO

# CONTRATO DE TRABALHO E TERMO ADITIVO

- IMPORTÂNCIA DO CÓDIGO DE CONDUTA
- CLÁUSULAS ESPECÍFICAS DE PRIVACIDADE E PROTEÇÃO DE DADOS
- ENTENDIMENTO JURISPRUDENCIAL



<https://portal.trt11.jus.br/index.php/main/2212-artigo-quem-odeia-a-justica-do-trabalho>



# Record of Processing Actives – ROPA

## Registro de Operações



ROPA – Record of Processing Actives

FONTE: Privacy Point

# ROPA



## ROPA - Record Of Processing Activities

PROCESSO	DESCRIÇÃO	AGENTE	BASES LEGAIS	DADOS TRATADOS	DADOS SENSÍVEIS	COMPARTILHAMENTO	ARMAZENAMENTO	MEDIDAS DE SEGURANÇA	TRANSFERÊNCIA INTERNACIONAL	CICLO DE VIDA
4. Fazer Plano de Ação	Aprender comunitária da área da Coordenação	Controlador	Execução do contrato.	Nome, Sim	Internas e Externas	Firewall, Antivirus	SIM	10 anos		
5. Realizar Avaliação Interna	Monitoramento das práticas internas e externas	Controlador	Execução do contrato	Nome, SIM	Internas e Externas	Firewall, antivirus	SIM	10 anos		
6. Realizar Avaliação e Pequeno Externo	Realizar avaliação das práticas inter e das outras	Controlador	Execução do contrato	Nome, Telefone particular, Telefone corporativo, E-mail	Internas e Externas	Antivirus, Firewall, Firewall, Firewall	SIM	10 anos		
7. Avaliar o Cancelar ou Bloquear os Alunos	Realizar avaliação das práticas inter e das outras	Controlador	Execução do contrato	Nome, CPF, Título de eleitor, CNH, Data de nascimento, Endereço, Telefone particular, E-mail	Internas e Externas	Antivirus, Firewall, Firewall, Firewall, políticar do backup	SIM	30 anos		
8. Consultar Contato Correntes	Expor os extratos de conta corrente para	Controlador	Prática da cidadania	Nome, CPF, Dados bancários, Telefone particular, Nome, OUTROS	Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	30 anos		
9. Conferir Ocorrência do Aluno	Geração de relatório de ocorrências	Controlador	Prática da cidadania	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	30 anos		
10. Contratar Câmbio	1º Ordem de remessa e cobrança	Controlador	Execução do contrato	Nome, CPF, CNH, Data de nascimento, Estado civil, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
11. Contratar e renovar provedor de serviços	Encaminhar minuta contratual para o DP Jurídico	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, Data de nascimento, Endereço, Telefone particular, E-mail corporativa, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
12. Contratar Orçamento Mensal	Contratar Orçamento Mensal, alimentar o Budget	Controlador	Prática da cidadania	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	5 anos		
13. Criar e Gerar Baleto de Cobrança	Criar e Gerar Baleto de Cobrança, Gerar balanço	Controlador	Execução do contrato	Nome, E-mail particular, E-mail corporativa, Nome, OUTROS	Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
14. Criar Planilha de Pagamento das Alunas	Criar forma de pagamento das alunas com cada	Controlador	Prática da cidadania	Nome, CPF, RG ou Passeport, Título de eleitor, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
15. Definir e Validar Orçamento	Validação do orçamento e acordo com o budget	Controlador	Prática da cidadania	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	5 anos		
16. Enviar Contrato de Prorrogação de Serviços	Enviar contrato para autorizar, via Partida do pagamento	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, Estado civil, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
17. Gerir Contar a Fazer	Pagamento via RPA - ocorre a informação	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, PIS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
18. Gerir Contar a Receber	Gerir das modalidades recebíveis e a receber	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
19. Gerir Fluxo de Pagamentos	Gerir fluxo de pagamento	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
20. Gerir Fluxo de Pagamentos	Aplicar regras de pagamento	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
21. Realizar Cobrança de Alunos Inadimplentes	Contar com os alunos inadimplentes, com a execução de pagamento, via internet banking, pagamentos	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
22. Realizar Prementes	Garar arquivamento de fiança	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, CNH, PIS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
23. Validar Balanço de Baleto de Cobrança de Matrícula	Garar arquivamento de fiança	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
24. Conferência de dados para a abertura fiscal	Verificar todos os dados para a abertura fiscal	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, CNH, PIS, CTPS, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	15 anos		
25. Contratar Recurso Humano CLT	Contratação do colaborador conforme	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
26. Contratar Professores	Contratação do professor conforme	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
27. Criar e/ou Atualizar as Matrículas do Contrato	Manter atualizada a matrícula de contrato	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	Não definida		
28. Contratar Mão-de-Obra Externa	Contratação do empregado em geral, profissional	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
29. Recrutar Contratado de Trabalho	Realização de desligamento das funções	Controlador	Execução do contrato	Nome, CPF, PIS, CTPS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
30. Fechar ou Reabrir o Extrato de Saída de Ponto	Controlar e aplicação durante a frequência das férias	Controlador	Execução do contrato	Nome, Características, Hora extra, Relatório de ponto	Internas	Antivirus, Firewall, Firewall, políticar do backup	SIM	30 anos		
31. Contratar Férias	Controlar e aplicação durante o período de férias conforme	Controlador	Execução do contrato	Nome, Dados bancários, Salário extra, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	30 anos		
32. Calcular Pagamento e Descontar das Férias	Realização do levantamento do valor das férias	Controlador	Execução do contrato	Nome, CPF, C攔nica médica, PIS, Déclar	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	30 anos		
33. Realizar Pagamento da Saláriada	Efetuar o pagamento das alíquotas calculadas	Controlador	Execução do contrato	Nome, Fone, Dados bancários, Saláriada, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	40 calendar		
34. Comprar Benefícios Alimentação e Vale	Realizar a aplicação durante o compra de benefícios	Controlador	Execução do contrato	Nome, Fone, Gastos, Estado civil, Naturalidade, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	35 anos		
35. Recrutar e Selecionar Funcionários	Realizar previsão de saída do novo funcionário	Controlador	Execução do contrato	Nome, Fone, Gabinete, Estado civil, Naturalidade, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
36. Definir Salários, Benefícios, Jornadas e Cargos	Realizar planejamento da mão de obra conforme	Controlador	Execução do contrato	Nome, Salário fixo, Produtividade, Remuneração	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
37. Realizar Matrícula para o Bacharelado	Realizar a matrícula para o Bacharelado	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, PIS, CTPS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
38. Realizar Matrícula para o Ensino Superior	Realizar a matrícula para o Ensino Superior	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, PIS, CTPS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
39. Envio de informações para a direção	Informar a data da chegada para a vistoria	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, PIS, CTPS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
40. Contratar instituição de ensino para contratar	Contratação do instituição de ensino para	Controlador conjunta	Execução do contrato	Nome, Fone, CPF, RG ou Passeport, Título de eleitor	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
41. Gerenciar comércio de Produtos	Gerenciar comércio de manutenção da máquina de fazer	Controlador	Execução do contrato	Nome, Fone, CPF, RG ou Passeport, PIS, CTPS, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
42. Gerenciar extrato e/ou das pessoas na SKEMA	O controle das pessoas e/ou das pessoas na SKEMA	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
43. Gerenciar Infraestrutura	Organização das áreas para o acesso ao ambiente	Controlador	Execução do contrato	Nome, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
44. Receber e Campar	Recebimento de materiais que foram comprados pela organização	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
45. Realizar Compra do Material de Expediente	Realizar compra de suprimentos para a organização	Controlador	Execução do contrato	Nome, Características, Telefone particular, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	15 anos		
46. Gerir Mão-de-Obra	Alinhar com o empregador para definir a limpeza	Controlador	Execução do contrato	Nome, Fone, RG ou Passeport, PIS, CTPS, Salário	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
47. Gerir Empregado do Ativismo	Horas precessas e folium contrato de comodato	Controlador	Execução do contrato	Nome, Fone, RG ou Passeport, E-mail corporativa	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
48. Contratar e acompanhamento da proteção do patrimônio	Assegurar a execução das proteções do patrimônio	Controlador	Execução do contrato	Nome, Fone, Voz, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	25 anos		
49. Avaliar Software, Hardwares e Provedores de Serviços	Assegurar o levantamento das avaliações	Controlador	Execução do contrato	Nome, Características, Telefone particular, Telefone	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	20 anos		
50. Instalar e Implementar Software e/ou Hardwares	Ex-precisa se atende a uma solicitação de um cliente	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, Nacionalidade, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
51. Capacitar Usuárias	Queridas usuárias que adquiriram novas ferramentas	Controlador	Execução do contrato	Nome, E-mail corporativa, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	5 anos		
52. Suprir Usuárias	Horas precessas e folium contrato de comodato	Controlador	Execução do contrato	Nome, Fone, RG ou Passeport, Dados bancários, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
53. Desenvolver Customizar Programas	Ex-precisa se facilitado para atender a demanda	Controlador	Execução do contrato	Nome, Fone, RG ou Passeport, Certificado do cliente	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	5 anos		
54. Bloquear o acesso de usuários deslogados	Bloquear o acesso de usuários deslogados	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	5 anos		
55. Gerenciar Contrato de Diagnóstico	Verificar se atendem prazos para dar contrato	Controlador	Legítima Interesse	Nome, Fone, CPF, RG ou Passeport, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
56. Gerenciar Contrato de Desenvolvimento	Verificar se atendem prazos para dar contrato	Controlador	Legítima Interesse	Nome, Fone, CPF, RG ou Passeport, Data de nascimento, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
57. Prender Contrato de Diagnóstico	Assinar contrato de SKEMA e fornecer o documento	Controlador	Execução do contrato	Nome, Fone, Outras dados biométricas, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
58. Atender Cliente Global	Responder a demanda, verificar com a disponibilidade	Controlador	Execução do contrato	Nome, Fone, Telefone particular, E-mail	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
59. Atender Cliente Internacional	Desenvolver e fornecer documentação para o cliente	Controlador	Execução do contrato	Nome, Fone, CPF, RG ou Passeport, CNH	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
60. Divulgar Companhias	Identificação de problemas e/ou dificuldades que a organização tem	Controlador	Execução do contrato	Nome, Fone, Voz, Naturalidade, Nacionalidade	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
61. Producir e Participar de Eventos	Organizar e executar encontro e/ou reuniões	Controlador	Legítima Interesse	Nome, Fone, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
62. Criar, Produzir e Validar Companhias	Identificação de problemas que a organização deve	Controlador	Execução do contrato	Nome, Fone, Voz	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
63. Vender Cursos	Entrar em contato com a candidata, realizar visitas	Controlador	Legítima Interesse	Nome, Fone, Voz, Outras dados biométricas, CPF, RG ou Passeport	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
64. Desenvolver Projeto e Branding	Identificação de problemas e/ou dificuldades que a organização tem	Controlador	Legítima Interesse	Nome, Fone, Voz	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
65. Atender ao Marketing Global	Receber e mandar a demanda do Marketing Global	Operador	Execução do contrato	Nome, Fone, Telefone particular, E-mail	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
66. Admitir Alunos Brasileiros	Prova e/ou prova de conhecimento para a candidata	Controlador	Execução do contrato	Nome, Fone, CPF, RG ou Passeport, Data de nascimento	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
67. Admitir Alunos Não-Brasileiros	Prova e/ou prova de conhecimento para a candidata	Controlador	Execução do contrato	Nome, CPF, RG ou Passeport, CNH, Data de nascimento	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	In determinado		
68. Admitir alunos para programar internacionais	Contratar com potenciais alunos para programar	Controlador	Execução do contrato	Nome, Fone, CPF, Data de nascimento	Internas e Externas	Antivirus, Firewall, Firewall, armazenamento em nuvem	SIM	In determinado		
69. Vendas e programação do programa de cursinhos	Entrar em contato com a turma para orientar os alunos	Controlador	Ex-precisa se o aluno é apto para cursar	Nome, Data de nascimento, Telefone particular, Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, anti-virus	SIM	10 anos		
70. Acompanhar Atualização da Acervo	A seguir a indicação da turma para cursinhos	Controlador	Execução do contrato	Nome, Dados de anotação, E-mail corporativa	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
71. Organizar Acervo	Se referir a organização das livrarias autorizadas	Controlador	Execução do contrato	Nome, OUTROS	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		
72. Treinar Colaboradores, Professores e Estudantes	Sumaritamente e detalhado dar palestras de coordenação	Controlador	Execução do contrato	Nome, E-mail corporativa	Internas e Externas	Antivirus, Firewall, Firewall, políticar do backup	SIM	10 anos		

# ITENS ROPA

- PROCESSO
  - DESCRIÇÃO
  - AGENTE
  - BASES LEGAIS
  - DADOS TRATADOS
  - DADOS SENSÍVEIS
  - COMPARTILHAMENTO
  - ARMAZENAMENTO
  - MEDIDAS DE SEGURANÇA
  - TRANSFERÊNCIA INTERNACIONAL
  - CICLO DE VIDA
  - JUSTIFICATIVA DE DESCARTE

Fonte ANPD



## **MODELO DE REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS PARA AGENTES DE TRATAMENTO DE PEQUENO PORTO (ATPP)**



# Ciclo de Vida de dados pessoais



# CICLO DE VIDA DOS DADOS PESSOAIS

## Ciclo de vida de dados

Área:  Processo:

Área	Processo	Dado	Tempo	Justificativa	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Inserção e cancelamento de contratos no sistema ContaAzul	Telefone corporativo	20 anos	art. 205 e 206 código civil	
Administrativo	Controle de horas e folgas dos funcionários	Hora extra	35 anos	art. 11 CLT	
Administrativo	Controle de horas e folgas dos funcionários	Hora extra	35 anos	art. 11 CLT	
Administrativo	Controle de horas e folgas dos funcionários	Hora extra	35 anos	art. 11 CLT	
Administrativo	Controle de horas e folgas dos funcionários	Hora extra	35 anos	art. 11 CLT	



# **Teste da hipótese de tratamento do interesse legítimo**

**LIA – LEGITIMATE INTEREST**

**ASSESSMENT**



Fonte: Privacy Point

# Legítimo

RESSE

## TESTE DOS QUATRO PASSOS

(LIA – Art. 37, caput, da LGPD)

**LEGITIMIDADE DO  
INTERESSE**  
(Art. 10, caput e  
inciso I da LGPD)

**NECESSIDADE**  
(10, §1º da LGPD)

**BALANCEAMENTO**  
(Art. 6º, I, 7º, IX e Art.  
10, II, da LGPD)

**SALVAGUARDA**  
(10, §2º e §3º da  
LGPD)

Finalidade  
Legítima

Minimização  
(menos intrusivo)

Legítima Expectativa  
(compatibilidade)

Transparência

Situação  
Concreta

Outras Bases Legais

Direitos e  
Liberdades  
Fundamentais

Mecanismos de  
Oposição (opt-out)

Adequação + Boa Fé  
(contexto)

Mitigação dos Riscos  
(e.g., anonimização)  
Outros Princípios PDP

## TESTE DO LEGÍTIMO INTERESSE

BASE LEGAL	DETALHES	ANOTAÇÕES
Legitimidade do Interesse (Art. 10, caput e <del>Inciso I</del> , da LGPD)	<b>FINALIDADE LEGÍTIMA</b> Criação de artes e posts para blog e mídias sociais com temas diversos e coberturas de eventos.	De acordo com o artigo 6º, I, é garantido ao titular dos dados o direito ao tratamento <u>adstrito</u> aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
	<b>SITUAÇÃO CONCRETA</b> A gestão da informação é importante para análises de riscos.	O fato é concreto e a utilização é necessária para o cumprimento do objeto social da empresa.
Necessidade (10, §1º, da LGPD)	<b>MINIMIZAÇÃO</b> (princípio da necessidade, uso de dados pessoais menos intrusivos)  Verificar se apenas os dados pessoais estritamente necessários para atingir a finalidade pretendida estão sendo processados. Verificar também se há outros tipos de dados menos intrusivos, disponíveis ao CONTROLADOR, que poderiam ser utilizados para atingir as mesmas finalidades.	Manter apenas dados estritamente necessários para o cumprimento da operação. De acordo com princípio da necessidade previsto no artigo 6º, III, que limita o 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.
	<b>OUTRAS BASES LEGAIS</b>  Verificar se alguma outra base legal, como consentimento, execução do contrato ou obrigação legal.	Conforme mapeamento, a base legal mais utilizada pela ADIAÚ DESENVOLVIMENTO WEB LTDA. é o da <u>EXECUÇÃO DE CONTRATOS</u> . O documento possui mais de 500 páginas e é bem completo.

	<b>LEGÍTIMA EXPECTATIVA</b> (compatibilidade do tratamento com a expectativa do titular) Verificar:  (i) se existe algum tipo de relação preestabelecida com o titular do dado de onde se possa inferir uma possível expectativa sua; ou (ii) se o homem médio, no contexto do tratamento dos dados, poderia vislumbrar que seus dados poderiam ser tratados para as finalidades descritas.	A expectativa é legítima e explícita na consecução do objeto social da <b>ADIAÚ DESENVOLVIMENTO WEB LTDA..</b>
	<b>DIREITOS E LIBERDADES FUNDAMENTAIS</b>  Verificar se algum direito básico do titular do dado, como direito de acesso, retificação, cancelamento e oposição, podem ser mitigados, além de liberdades fundamentais, como liberdade de expressão, locomoção, associação e outras previstas, não serão impactadas de forma desproporcional ao ponto de prejudicar o indivíduo de forma não autorizada.	Não há violação de direitos fundamentais.
	<b>TRANSPARÊNCIA</b>  Salvaguardas (10, §2º e §3º da <u>LGPD</u> ) Quais são as medidas e instrumentos empregados para garantir os direitos dos titulares dos dados e evitar que seus dados sejam eventualmente utilizados de forma indevida.	O mapeamento realizado demonstra todos os processos em que há o tratamento de dados pessoais. Ainda, existe o <u>CANAL DE PROTEÇÃO DE DADOS</u> que está disponível para os titulares dos dados.
	<b>MECANISMOS DE OPOSIÇÃO (opt-out)</b>  Forma como o titular dos dados pode se opor ao tratamento dos seus dados, caso não concorde ou se o tratamento estiver em desconformidade com a legislação.	Canal de Proteção de Dados

Luiz Felipe  
EXC - Exclusive Seguros

- Administração >
- Data Mapping >
- ROPA >
- Gestão eletrônica de documentos >
- Plano de ação
- Ciclo de vida de dados
- Gestão de incidentes
- Formulários
- Ouvidoria

## LIA - Teste de interesse legítimo

Processo	Data	Versão	Arquivo

### Processos ainda sem LIA

Prospecção de novos seguros através de dados enviados pelas concessionárias  
Prospecção de novos seguros através de representante na concessionária  
Prospecção de novos seguros para já clientes  
Pedidos de renovação  
Comercialização de seguros massificados

# Relatório de IMPACTO DE DADOS

**Art. 38.** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

**Parágrafo único.** Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Fonte: Privacy Point



# RIPD

## *Data Mapping*

com base nos  
conceitos da  
LGPD (Lei Geral de  
Proteção de Dados)

Dados coletados no período de  
01/04/2023 a 22/12/2023

Elaborado por  
Luiz Felipe



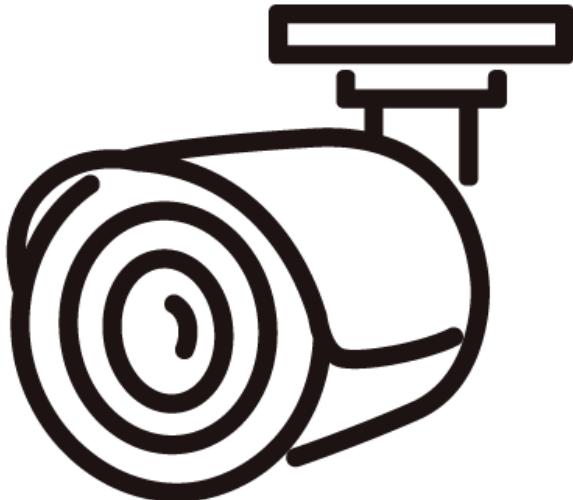
# RIPD

**RELATÓRIO DE IMPACTO**

**À PROTEÇÃO DE DADOS PESSOAIS**

**Uso de Câmeras de Monitoramento e Coleta de Dados**

**Biométricos**



**Ambiente monitorado por coleta de imagens  
em conformidade com a LGPD – Art.11, “g”.**

**Finalidade:** Segurança pessoal e patrimonial

**Controlador:** SKEMA Business School

**Encarregado de Dados:** dpo@privacypoint.com.br

**CNPJ:** 29.809.849/0001-92

**Environment monitored by image collection in  
accordance with the General Data Protection  
Law (LGPD) - Art.11, “g”.**

**Purpose:** Personal and property security

**Controller:** SKEMA Business School

**Data Protection Officer:** dpo@privacypoint.com.br

**CNPJ:** 29.809.849/0001-92

FONTE: PRIVACY POINT

# RIPD

**RELATÓRIO DE IMPACTO  
À PROTEÇÃO DE DADOS PESSOAIS  
UTILIZAÇÃO DE NOVO SISTEMA  
POWER BI**

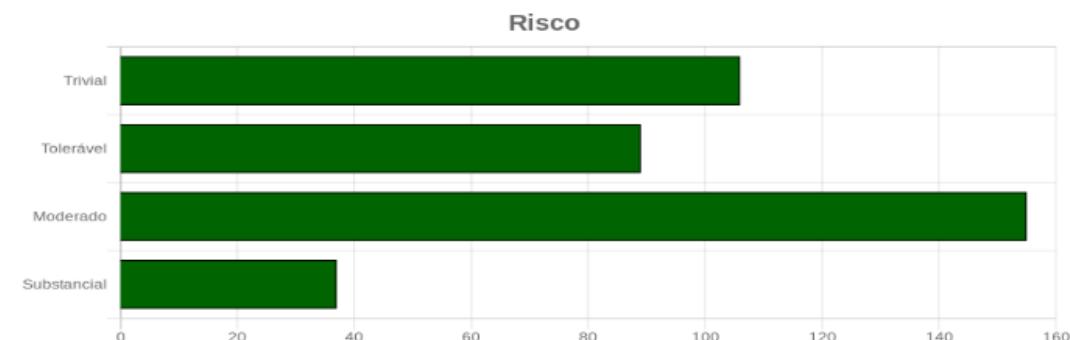
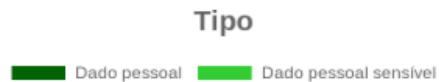
# Avaliação de tratamento de dados

## ADIAU

privacy  
point

### RESUMO DO TRATAMENTO CONSIDERANDO TODAS AS ÁREAS

Total de processos mapeados: 90  
Total de tipo de dados: 4



RIPD

## Avaliação de tratamento de dados

ADIAU

priv<sup>acy</sup>  
point

### DETALHAMENTO DOS DADOS TRATADOS

Descrição do dado	Total de processos	Compartilhamento		Armazenamento em nuvem	Política de descarte	Maior risco identificado
		Externo	Interno			
Nome	5	Sim	Sim	Não	Não	Moderado
Telefone corporativo	3	Sim	Sim	Não	Não	Trivial
E-mail corporativo	4	Sim	Sim	Não	Não	Trivial
Endereço	2	Sim	Sim	Não	Não	Moderado
CPF	6	Sim	Sim	Não	Não	Moderado
CTPS	3	Sim	Sim	Não	Não	Moderado
Data de nascimento	5	Sim	Sim	Não	Não	Moderado
Dados bancários	2	Sim	Sim	Não	Não	Moderado
Conta FGTS	2	Sim	Sim	Não	Não	Moderado
Salário base	1	Sim	Sim	Não	Não	Tolerável
Benefícios	1	Sim	Sim	Não	Não	Tolerável
Hora extra	2	Sim	Sim	Não	Não	Tolerável
Cargo	2	Sim	Sim	Não	Não	Trivial
Atestados médicos	1	Sim	Sim	Não	Não	Substancial
Licenças	1	Sim	Sim	Não	Não	Substancial
Data de admissão	2	Sim	Sim	Não	Não	Trivial
Regime de trabalho	1	Sim	Sim	Não	Não	Trivial
Registro de entrada e saída	2	Sim	Sim	Não	Não	Tolerável
Foto	6	Sim	Sim	Não	Não	Substancial
Voz	4	Sim	Sim	Não	Não	Substancial
Telefone particular	2	Sim	Sim	Não	Não	Tolerável
E-mail particular	2	Sim	Sim	Não	Não	Tolerável
RG ou Passaporte	2	Sim	Sim	Não	Não	Moderado
CNII	2	Sim	Sim	Não	Não	Moderado
PIS	2	Sim	Sim	Não	Não	Moderado

# TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS



# Transferência INTERNACIONAL DE DADOS

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

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- A. cláusulas contratuais específicas para determinada transferência;
- B. cláusulas-padrão contratuais;
- C. normas corporativas globais;
- D. selos, certificados e códigos de conduta regularmente emitidos;

**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:

(...).

**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.



# Cláusulas Contratuais

## PADRONIZADAS

A Autoridade Supervisora pode adotar cláusulas contratuais-padrão para o contrato vinculante entre o controlador e o processador e, se apropriado (por exemplo, com autorização prévia por escrito do controlador), entre o **CONTROLADOR** e o **OPERADOR**.

# REQUISITOS CLÁUSULA CONTRATUAL PADRÃO

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>i. Definições básicas e objeto</li><li>ii. Transferências posteriores</li><li>iii. Parte designada</li><li>iv. Finalidade do contrato e definições</li><li>v. Legislação aplicável e fiscalização da ANPD</li><li>vi. Interpretação</li><li>vii. Possibilidade de adesão de terceiros</li><li>viii. Obrigações gerais das partes</li><li>ix. Dados sensíveis</li><li>x. Dados de crianças e adolescentes</li></ul> | <ul style="list-style-type: none"><li>xi. Transparência</li><li>xii. Direitos dos titulares</li><li>xiii. Comunicação de Incidente de Segurança</li><li>xiv. Responsabilidade e resarcimento de danos</li><li>xv. Salvaguarda para transferência posterior</li><li>xvi. Notificação de Solicitação de Acesso</li><li>xvii. Término do tratamento e eliminação dos dados</li><li>xviii. Segurança no tratamento dos dados</li><li>xix. Descumprimento do contrato</li><li>xx. Legislação aplicável e Eleição de foro</li></ul> |
|--|---|

FONTE: <https://www.gov.br/anpd/pt-br/assuntos/noticias/MinutaRegulamentoTID.pdf>

# BCR – Binding Corporate Rules

## REGULAMENTO EMPRESARIAL

Um grupo de empresas, ou um grupo de empresas envolvidas numa atividade econômica conjunta, deve poder utilizar as regras empresariais vinculantes aprovadas para as suas transferências internacionais da União para organizações pertencentes ao mesmo grupo de empresas ou grupo de empresas uma atividade econômica conjunta, desde que tais regras corporativas incluam todos os princípios essenciais e direitos aplicáveis para garantir as salvaguardas apropriadas para transferências ou categorias de transferências de dados pessoais. Fonte: Privacy Point



Código de Conduta  
atualizado com a LGPD



Políticas de Privacidade  
e Segurança da  
Informação



Depende de  
chancela da  
ANPD

Fonte: Privacy Point



# REQUISITOS NORMAS CORPORATIVAS GLOBAIS

- (i) comprometimento em adotar políticas e processos que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- (ii) seja aplicável a todo o conjunto de dados pessoais objetivo da coleta;
- (iii) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- (iv) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade e à proteção de dados pessoais;
- (v) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- (vi) esteja integrado à estrutura geral de governança, bem como estabeleça e aplique mecanismos de supervisão internos e externos; (vi) conte com planos de resposta a incidentes e remediação; e (viii) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas

# REQUISITOS NORMAS CORPORATIVAS GLOBAIS

- (i) especificação das transferências internacionais de dados para as quais o instrumento se aplica;
- (ii) identificação dos países para os quais os dados são transferidos;
- (iii) estrutura do grupo econômico;
- (iv) determinação da natureza vinculante da norma corporativa global para todos os membros do grupo econômico;
- (v) delimitação de responsabilidades pelo tratamento;
- (vi) indicação dos direitos dos titulares aplicáveis e os meios para o seu exercício;
- (vii) regras sobre o processo de revisão e,
- (viii) revisão de comunicação à ANPD em caso de alterações nas garantias apresentadas.

[https://www.gov.br/anpd/pt-br/assuntos/noticias/AIR\\_Transferencias\\_VF.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/AIR_Transferencias_VF.pdf)



<https://nasatecnologia.com.br/tranferencia-internacional-de-dados-lgpd/>

# IMPORTANTE

- Uma pesquisa recente realizada na União Europeia concluiu que “as Cláusulas-Padrão Contratuais (CPC) são de longe o mecanismo mais amplamente utilizado para transferências de dados. Dentre as empresas pesquisadas, estima-se que 85% utilizam CPCs, enquanto outros mecanismos de transferência, como decisões de adequação, normas corporativas globais (BCRs) ou derrogações (por exemplo, consentimento) representam pouco mais de 5% das transferências.”

DIGITAL EUROPE. Schrems II: Impact Survey Report, 2020, p. 5. Disponível em:

[https://digital-europe-website-v1.s3.frpar.scw.cloud/uploads/2020/11/DIGITALEUROPE\\_Schrems-II-Impact-Survey\\_November-2020.pdf](https://digital-europe-website-v1.s3.frpar.scw.cloud/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf).



# *PRIVACY BY DESIGN E PRIVACY BY DEFAULT*

# PRIVACY BY DESIGN E PRIVACY BY DEFAULT

## PRIVACY BY DESIGN “Ann Cavoukian”

- Uma abordagem para projetos que promove a conformidade com a privacidade e proteção de dados desde o início de um projeto.
- Usuário no centro da concepção do projeto.
- Fonte: ICO

## PRIVACY BY DEFAULT

- A proteção by design é expandida para incluir "por padrão", que insiste em que a organização assegure que todos os projetos levarão sempre em conta a proteção de dados.
- Privacidade & Proteção de Dados por PADRÃO

Fonte: Livro EU General Data Protection Regulation(GDPR).  
AnImplementationand ComplianceGuide, ITGP

# PRIVACIDADE POR PADRÃO

- **GDPR art. 25(2)**
- “O controlador aplica **medidas técnicas e organizacionais** para assegurar que, **por padrão**, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais coletados, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.”

## EXEMPLOS

- Minimização do processamento
- Pseudonimização
- A realização de uma RPD

# CONHEÇA OS 7 PRINCÍPIOS DO PRIVACY BY DESIGN

<https://www.gepcompliance.com.br/blog/privacy-by-design-saiba-como-adequar-o-seu-produto-a-lgpd/>





PUC Minas

# VAZAMENTO DE DADOS

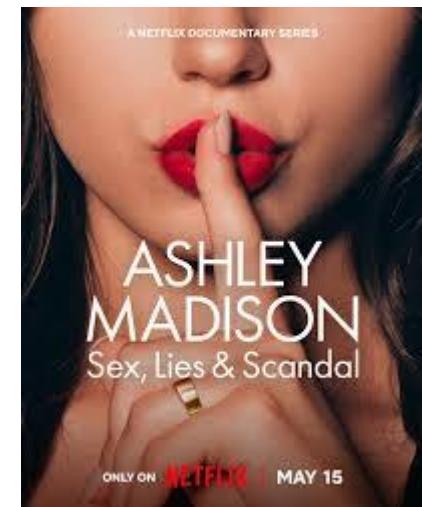
# VAZAMENTO DE DADOS

- Perda de Reputação
- Perda de Credibilidade
- Perda de Confiança
- Induz falta de cuidado
- Vulnerabilidade
- Pe
- Queda do valor da ação em caso de S/A

Fonte Netflix

## EXEMPLOS

- ❖ NETSHOES
- ❖ BANCO INTER
- ❖ DROGARIA ARAÚJO
- ❖ Escritório Advocacia BH
- ❖ ASHLEY MADSON

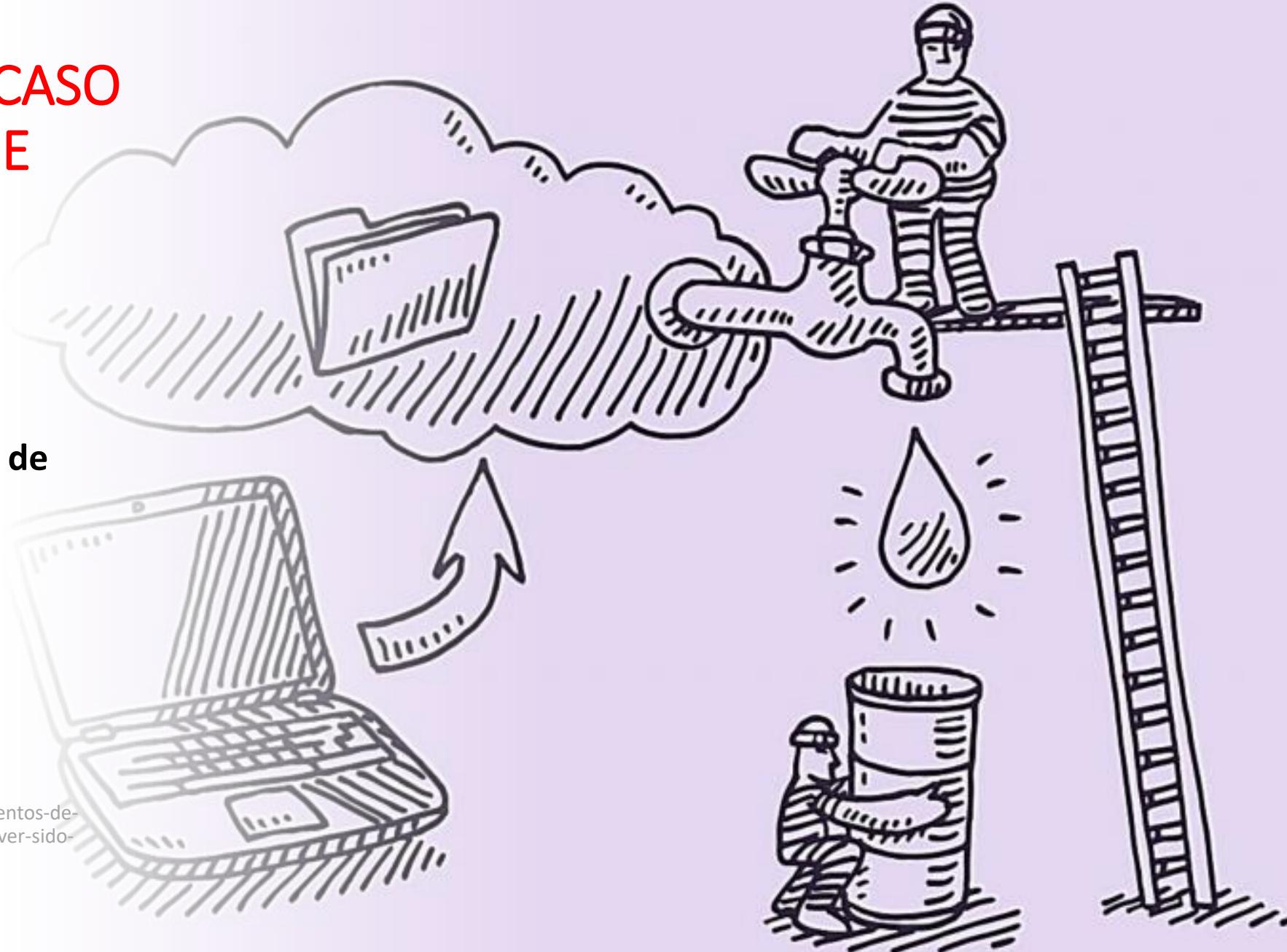


# O QUE FAZER EM CASO DE VAZAMENTO DE DADOS

- **ETAPAS**

- 1. Desenvolver um plano de ação**
- 2. Monitorar eventos**
- 3. Incidente de violação**
- 4. Relatar**
- 5. Resolver e recuperar**

Fonte: <https://idec.org.br/dicas-e-direitos/vazamentos-de-dados-pessoais-dicas-para-evitar-e-reclamar-se-tiver-sido-afetado>



# ART. 48 LGPD – PRAZO RECOMENDADO ANPD

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.

## ➤ ANPD

*“Para preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, recomenda-se que a comunicação seja feita o mais breve possível, em até 2 (dois) dias úteis da ciência do fato.”*

FONTE: [https://www.gov.br/anpd/pt-br/canais\\_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis](https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis)



# PLANO DE RESPOSTA DE VIOLAÇÕES DE DADOS



Luiz Felipe  
Administração Geral

- Luis Felipe
- Administração
- Data Mapping
- ROPA
- Gestão eletrônica de documentos
- Plano de ação
- Ciclo de vida de dados
- Gestão de incidentes
- Formulários

## Novo incidente

Data

dd/mm/aaaa



Área

Selecionar a área

Processo:

Selecionar o processo



Responsável

Selecionar responsável

Total de titulares impactados

Escolha



Classificação do impacto

Escolha



Descrição do incidente:



Ações realizadas:



Titulares informados?

Sim  Não

Anexar documento de comunicação:

Escolher arquivo Nenhum arquivo escolhido

ANPD informada

Sim  Não



# ANPD

Autoridade  
Nacional de  
Proteção de Dados

## Formulário de Comunicação de Incidente de Segurança com Dados Pessoais



### Dados do Controlador

Razão Social / Nome:	*****S/A			
CNPJ/CPF:	*****			
Endereço:	*****			
Cidade:	Belo Horizonte	Estado:	Minas Gerais	
CEP:	30110-042			
Telefone:	31-3330-3080	E-mail:	<a href="mailto:DPO@PRIVACYPOINT.COM.BR">DPO@PRIVACYPOINT.COM.BR</a>	
Declara ser Microempresa ou Empresa de Pequeno Porte:	<input type="checkbox"/>	Sim	<input checked="" type="checkbox"/>	Não
Declara ser Agente de Tratamento de Pequeno Porte:	<input type="checkbox"/>	Sim	<input checked="" type="checkbox"/>	Não

Tipo de Comunicação	
<input type="checkbox"/> · Completa	Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.
<input type="checkbox"/> · Preliminar	Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a comunicação aos titulares ainda não foi realizada. A complementação deverá ser encaminhada em até 30 dias corridos da comunicação preliminar.
<input checked="" type="checkbox"/> · Complementar	Complementação de informações prestadas em comunicação preliminar. A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

➤→ A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Avaliação do Risco do Incidente	
<input type="checkbox"/> · O incidente de segurança pode acarretar risco ou dano relevante aos titulares.	
<input checked="" type="checkbox"/> · O incidente não acarretou risco ou dano relevante aos titulares. ( <b>Comunicação Complementar</b> )	
<input type="checkbox"/> · O risco do incidente aos titulares ainda está sendo apurado. → ..... ( <b>Comunicação Preliminar</b> )	
<b>Justifique, se cabível, a avaliação do risco do incidente:</b>	

## Avaliação do Risco do Incidente

- O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
- O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**
- O risco do incidente aos titulares ainda está sendo apurado. → ..... **(Comunicação Preliminar)**

### Justifique, se cabível, a avaliação do risco do incidente:

Vazamento de dados dos funcionários em uma lista interna do Departamento Pessoal contendo nome, e-mail, cargo e remuneração. Vazamento oriundo de falha na autenticação. Pequeno risco aos titulares afetados, uma vez que o terceiro que invadiu o sistema de e-mail do Controlador gostaria de ter acesso às remunerações que são pagas aos Gestores do Hospital.

## Da Ciência da Ocorrência do Incidente

### Por qual meio se tomou conhecimento do incidente?

- Identificado pelo próprio controlador.
- Notificação do operador de dados.
- Denúncia de titulares/terceiros.
- Notícias ou redes sociais.
- Notificação da ANPD.
- Outro: \_\_\_\_\_

### Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:

## Da Tempestividade da Comunicação do Incidente

Informe as seguintes datas, sobre o incidente:

Quando ocorreu: 28/03/2024

Quando tomou ciência: 01/04/2024

Quando comunicou à ANPD: 03/04/2024

Quando comunicou aos titulares: 03/04/2024

Justifique, se cabível, a não realização da comunicação completa à ANPD e aos titulares de dados afetados no prazo sugerido de 2 (dois) dias úteis após a ciência do incidente:

O incidente ocorreu no feriado da Páscoa. O Controlador enviou a Comunicação Preliminar em dois dias úteis após a ciência do fato.

Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:

## Da Comunicação do Incidente aos Titulares dos Dados

Os titulares dos dados afetados foram comunicados sobre o incidente?

## Da Comunicação do Incidente aos Titulares dos Dados

### • Os titulares dos dados afetados foram comunicados sobre o incidente?

- Sim.  Não, por não haver risco ou dano relevante a eles.
- Não, mas o processo de comunicação está em andamento.  Não, vez que o risco do incidente ainda está sendo apurado. (comunicação preliminar)

### Se cabível, quando os titulares serão comunicados sobre o incidente?

□

### De que forma a ocorrência do incidente foi comunicada aos titulares?

- Comunicado individual por escrito. ¶ (mensagem eletrônica / carta / e-mail / etc.)  Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
- Comunicado individual por escrito com confirmação de recebimento. ¶ (mensagem eletrônica / carta / e-mail / etc.)  Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (especifique abaixo)
- Outra: \_\_\_\_\_  Não se aplica.

### Descreva como ocorreu a comunicação:

Foi enviado um comunicado por e-mail para cada colaborador que teve seus dados pessoais vazados. O Controlador tem cópia desse e-mail.

## Impactos do Incidente Sobre os Dados Pessoais

### De que formas o incidente afetou os dados pessoais?

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Confidencialidade | Houve acesso não autorizado aos dados, violando seu sigilo.                    |
| <input type="checkbox"/> Integridade                  | Houve alteração ou destruição de dados de maneira não autorizada ou acidental. |
| <input type="checkbox"/> Disponibilidade              | Houve perda ou dificuldade de acesso aos dados por período significativo.      |

### Se aplicável, quais os tipos de dados pessoais sensíveis foram violados?

- |   |  |  |
|---|--|--|
| <input type="checkbox"/> Origem racial ou étnica. | <input type="checkbox"/> Convicção religiosa.  | <input type="checkbox"/> Opinião política. |
| <input type="checkbox"/> Referente à saúde.       | <input type="checkbox"/> Biométrico.   | <input type="checkbox"/> Genético.         |
| <input type="checkbox"/> Referente à vida sexual. | <input type="checkbox"/> Filiação a organização sindical, religiosa, filosófica ou política. |  |

### Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Não houve vazamento de dados pessoais sensíveis.

### Quais os demais tipos de dados pessoais violados?

Descrição do Incidente	
<b>Qual o tipo de incidente? (Informe o tipo mais específico):</b>	
<input type="checkbox"/> Sequestro de Dados ( <u>ransomware</u> ) sem transferência de informações. <input checked="" type="checkbox"/> Exploração de vulnerabilidade em sistemas de informação. <input checked="" type="checkbox"/> Roubo de credenciais / Engenharia Social. <input type="checkbox"/> Publicação não intencional de dados pessoais. <input type="checkbox"/> Envio de dados a destinatário incorreto. <input type="checkbox"/> Negação de Serviço (DoS). <input type="checkbox"/> Perda/roubo de documentos ou dispositivos eletrônicos. <input type="checkbox"/> Falha em equipamento (hardware). <input type="checkbox"/> Outro tipo de incidente cibernético.	<input type="checkbox"/> Sequestro de dados ( <u>ransomware</u> ) com transferência e/ou publicação de informações. <input type="checkbox"/> Vírus de Computador / Malware. <input type="checkbox"/> Violação de credencial por força bruta. <input type="checkbox"/> Divulgação indevida de dados pessoais. <input type="checkbox"/> Acesso não autorizado a sistemas de informação. <input type="checkbox"/> Alteração/exclusão não autorizada de dados. <input type="checkbox"/> Descarte incorreto de documentos ou dispositivos eletrônicos. <input type="checkbox"/> Falha em sistema de informação (software). <input type="checkbox"/> Outro tipo de incidente não cibernético.
<b>Descreva, resumidamente, como ocorreu o incidente:</b>	
<p>Um terceiro, desconhecido do Controlador, acessou indevidamente o e-mail de uma funcionária do Departamento Pessoal do Hospital Socor S/A e enviou um e-mail para 35 (trinta e cinco) colaboradores e 06 (seis) ex-funcionários, contendo nome, e-mail e remuneração dos destinatários da aludida mensagem eletrônica. Sabe-se que o terceiro utilizou o IP 181.77.21.85 e que o e-mail foi encaminhado fora das dependências do Controlador. O IP 181.77.21.85 é provido pela TIM S/A. O terceiro tinha o claro objetivo de obter informação do valor da remuneração dos Gestores do Hospital.</p>	
<b>Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):</b>	
<p>A colaboradora que teve seu e-mail e senha obtidos por via de engenharia social. Somente uma planilha do RH</p>	



**PUC Minas**