DEFENSORIA PÚBLICA
ESTADO DO RIO GRANDE DO SUL

Entendendo a

Lei Geral de Proteção de Dados

Um guia breve e simples produzido pela Defensoria Pública do Estado do Rio Grande do Sul sobre a Lei nº 13.709/2018

Comissão
sobre a LGPD

Abril 2021

COMISSÃO SOBRE A LGPD

ALEX SCHNEIDER ZIS

CRISTIANO BERTUOL

DANIELA CENCI LIMA

EDUARDO PEREIRA LIMA ZANINI

RICARDO JOSÉ CALDAS HERBERT

ROGÉRIO SOUZA COUTO

TIAGO RODRIGO DOS SANTOS

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTORA
15/04/2021	1.0	PRIMEIRA VERSÃO DO GUIA	DANIELA CENCI LIMA

Conteúdo

4 A IMPORTÂNCIA DOS DADOS

6 A LEI

7 A PROTEÇÃO NA DPE/RS

8 OS PRINCIPAIS CONCEITOS

10 OS FUNDAMENTOS

10 A APLICAÇÃO

11 OS PRINCÍPIOS

12 AS BASES LEGAIS

15 OS DADOS SENSÍVEIS

15 AS CRIANÇAS E OS ADOLESCENTES

16 OS DIREITOS DOS TITULARES

17 A TRANSPARÊNCIA

17 O FIM DO TRATAMENTO

18 AS BOAS PRÁTICAS

18 A PRIVACIDADE POR DESIGN

19 A SEGURANÇA

20 AS RESPONSABILIDADES

20 AS PENALIDADES

21 A AUTORIDADE NACIONAL

22 AS DICAS DE SEGURANÇA

24 AS LEIS RELACIONADAS

24 PARA CONHECER MAIS

25 O CONTATO DA DPE/RS

A Importância dos Dados

Por que os dados são importantes?

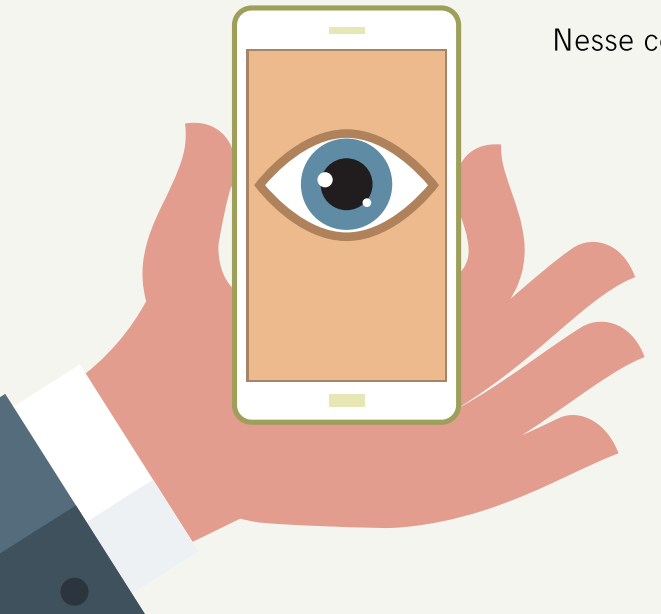
Nossos dados estão por todos os lugares. Fornecemos para receber promoções em lojas, para comprar remédios na farmácia, para receber um serviço em um órgão público, para poder realizar um curso técnico. Também na internet, em troca da utilização gratuita de aplicativos e redes sociais, fornecemos nossos dados, tanto pessoais quanto de interesses.

Com base nos dados coletados, as empresas podem traçar nossas preferências e perfis de consumo - inclusive podem fazer previsões sobre o nosso comportamento - ou mesmo identificar melhores locais para investir. Além dos proveitos para o setor privado, os dados também geram significativos ganhos sociais e econômicos para o setor público. Os dados permitem reconhecer, filtrar e extrair valor de informações sobre políticas públicas para tomar melhores decisões. Fornecem ainda novas percepções em tempo real e previsões sobre onde agir para lidar com riscos e identificar novas oportunidades.

Os grandes conjuntos de dados - pessoais e não pessoais - formam uma cadeia de valor e estão se tornando um ativo fundamental na economia, estimulando novos setores, processos e produtos e criando significativas vantagens competitivas.

Por que devem ser protegidos?

O crescente valor dos dados tem sido acompanhado pela preocupação acerca da "extração" a qualquer custo, bem como da vulnerabilidade dos cidadãos por causa de usos inadequados, abusos flagrantes ou mesmo consequências indesejadas. Muitos dados têm sido usados, compartilhados, vendidos ou vazados com pouco - ou nenhum - envolvimento das pessoas mais afetadas e com pouca - ou nenhuma - consciência ética por parte das organizações responsáveis *.



Nesse contexto, a proteção de dados pessoais tem por objetivo manter nossos dados seguros e garantir que sejam usados de maneira justa e responsável.

É preciso construir confiança entre pessoas e organizações, reconhecendo o direito de um indivíduo de ter controle sobre suas informações pessoais - mesmo quando são mantidas por terceiros - e encontrando um equilíbrio entre esses direitos individuais e os interesses da sociedade.

* Texto de Geoff Mulgan e Vincent Straub chamado 'O Novo Ecossistema da Confiança' Disponível em https://nesta.org.uk/blog/new-ecosystem-trust/

Um Exemplo Prático

Cláudia está vasculhando sua bolsa em busca de seu celular no ônibus a caminho de casa, após fazer uma entrevista para um novo trabalho em uma rede de farmácias. Cláudia se acomoda em um assento e abre o aplicativo da 'Seu Carro Novo Financeira', local onde ela fez um financiamento para comprar o próprio veículo no ano passado. "Em breve vou poder voltar para casa dirigindo meu carro", pensa ela, fazendo login no aplicativo e checando as parcelas a pagar e os juros. Cláudia está desempregada há poucos meses e atrasou o pagamento do financiamento, mas tem esperanças de conseguir o novo emprego e, com a entrada do salário, deixar de ser uma "má pagadora". Chegando em casa, Cláudia verifica sua conta de e-mail. Surpresa ao ver o nome do aplicativo da instituição financeira que ela estava usando, ela abre a mensagem para descobrir que sua conta foi comprometida. Seus dados e de mais de 600 mil brasileiros foram vazados. Assustada e irritada, Cláudia exclui rapidamente o aplicativo de seu telefone e decide que acompanhará as movimentações do financiamento à forma antiga, presencialmente ou por telefone. Semanas depois, Cláudia ainda não pode ter certeza de que seus dados pessoais e financeiros não foram vendidos a empresas do setor de comércio eletrônico. Já foram vendidos para companhias de telecomunicações - ela sabe disso por causa dos anúncios que continuam aparecendo em seu Instagram e porque tem recebido insistentes ligações com ofertas de São Paulo. Mas e se a empresa onde está buscando trabalho, de alguma forma, conseguisse acesso aos dados e soubesse de sua dívida, isso poderia colocar a chance do novo emprego em risco?

Na verdade, os dados sobre as parcelas do financiamento de Cláudia não são só o que essas empresas procuram, mas sim o "entulho digital" que ela deixa para trás quando lê notícias ou assiste vídeos, faz postagens sobre a busca de trabalho ou até mesmo pesquisas de ofertas de supermercados. Esses metadados são usados para fazer inferências que combinadas criam um perfil de Cláudia - sua "gêmea digital" - cujo comportamento potencial é cuidadosamente rastreado, analisado e marcado de acordo. Algumas empresas apostam, então, em como a "Cláudia digital" se comportará em tais cenários e estão lucrando com Cláudia sem seu conhecimento ou consentimento. São esses usos secundários de metadados sobre os quais Cláudia - e o resto de nós que usa aplicativos, plataformas e serviços online "gratuitos" - não tem nenhum controle.

Adaptado do informe elaborado pela Digital Future Society
'Rumo a uma melhor governança de dados para todos: ética de dados e privacidade na era digital'
Disponível em https://digitalfuturesociety.com/

A Lei Geral de Proteção de Dados

A crescente consciência pública em torno do potencial valor das inovações baseadas em dados, bem como a necessidade de preservar os direitos e fortalecer a confiança dos titulares, impulsionaram o desenvolvimento de um quadro jurídico sólido em termos de proteção de dados.

Isso porque, para obter os máximos benefícios econômicos e sociais do tratamento dos dados, os cidadãos, as empresas e os demais atores envolvidos devem estar seguros de que todo e qualquer uso ou compartilhamento de dados pessoais estará sujeito à plena observância de regras claras que disciplinem um tratamento responsável.

Até o presente momento, 128 países ao redor do mundo já adotaram legislação para garantir a proteção de dados e a privacidade.

No Brasil, houve a publicação da Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD dispõe sobre o tratamento de dados pessoais, tanto nos meios físicos quanto digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade.

A lei introduz uma série de novos direitos que asseguram maior transparência, privacidade e segurança. Dá protagonismo e poder às pessoas sobre o uso de seus próprios dados. E também estabelece orientações gerais, responsabilidades e obrigações a quem faz uso dos dados.

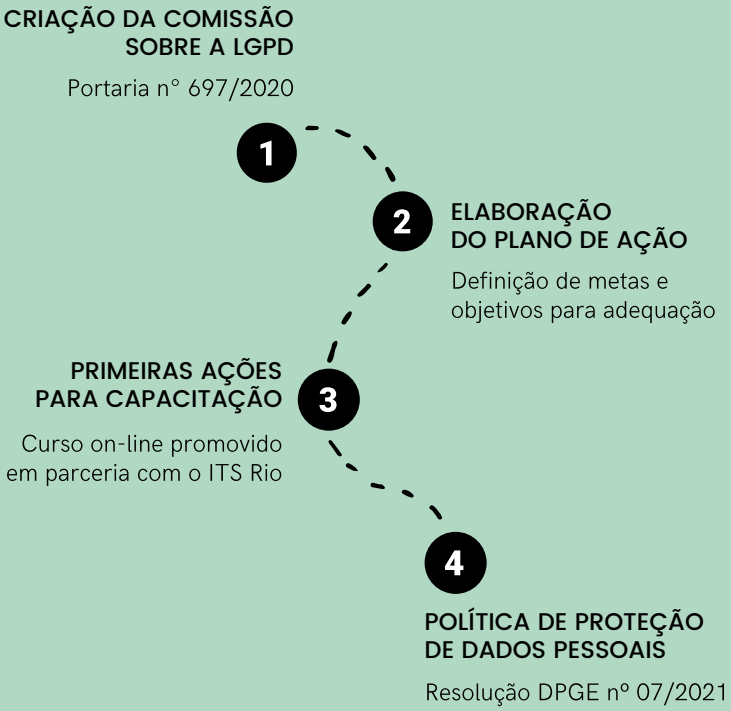
O presente guia ajuda a entender o conteúdo da lei, através de uma linguagem mais simples e de exemplos concretos. Por isso, alguns termos mais técnicos foram adaptados, devendo prevalecer sempre o texto da lei.

A Proteção de Dados na Defensoria Pública do Estado do Rio Grande do Sul

A Defensoria Pública do Estado do Rio Grande do Sul entende necessário estabelecer uma relação de confiança, de proteção e de privacidade com relação aos dados dos cidadãos - tanto daqueles que usam seus serviços quanto daqueles que trabalham para a instituição.

Por isso, a Defensoria Pública assume o compromisso de adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Também se compromete a desenvolver ações voltadas à governança de dados e a assegurar a resposta adequada aos riscos, ameaças e desafios relacionados.

Para atingir esses objetivos, o Plano de Ação para adequação estabelece as seguintes frentes: Transparência e Comunicação • Capacitação • Registro de Tratamento de Dados • Direitos dos Titulares • Contratos e Instrumentos Congêneres • Segurança da Informação • Estrutura Organizacional.



POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS
- ARTIGO 1º DA PPDP -

Nossa Política de Proteção de Dados Pessoais (PDPP) foi publicada em março de 2021. Tem como objetivos: (1) estabelecer normas, princípios e procedimentos para nortear o tratamento de dados pessoais, em meios físicos e digitais, na Defensoria Pública do Estado do Rio Grande do Sul, (2) garantir a efetiva proteção da privacidade dos titulares e (3) definir papéis e diretrizes iniciais para obtenção da gradual conformidade institucional ao previsto na LGPD.

As disposições da Política são aplicáveis a todo o conjunto de dados pessoais que estejam sob o controle da Defensoria Pública e regulam o relacionamento com os usuários de seus serviços e com os membros, servidores, estagiários, fornecedores e quaisquer terceiros.

COMITÊ GESTOR DE PROTEÇÃO DE DADOS
- ARTIGO 29 DA PPDP -

O Comitê Gestor de Proteção de Dados, com caráter multidisciplinar e multissetorial, será responsável, de forma duradoura, pelo desenvolvimento e pela gestão do programa de governança e proteção de dados, com vistas também à adequação institucional às disposições da LGPD.

Dentre outras atribuições, o Comitê ajudará a colocar em prática ações voltadas à proteção de dados pessoais, à privacidade e a medidas de segurança na Defensoria Pública, poderá sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais e promoverá o conhecimento das normas e das políticas públicas na área.

ACESSE AQUI A POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Principais Conceitos

ARTIGO 5º DA LGPD

O QUE SÃO DADOS PESSOAIS?

Toda informação relacionada a uma pessoa que a identifique ou a torne identificável. Ou seja, que permite saber quem é a pessoa.

Também podem ser considerados dados pessoais aqueles usados para formar um perfil de comportamento de determinada pessoa, se identificada.

EXEMPLOS nome • número de inscrição no Registro Geral (RG) ou no Cadastro de Pessoas Físicas (CPF) • endereço residencial • data de nascimento • foto de identificação 3x4 • placa numérica do carro • endereço de IP • fatores específicos sobre sua aparência • aspectos específicos de sua personalidade • histórico de compras • localização geográfica • ou preferências de consumo.

O QUE É TRATAMENTO?

Tratamento de dados pessoais é toda e qualquer ação realizada com os dados pessoais.

EXEMPLOS coleta • produção • recepção • classificação • utilização • acesso • reprodução • transmissão • distribuição • processamento • arquivamento • armazenamento • eliminação • avaliação ou controle da informação • modificação • comunicação • transferência • difusão • extração dos dados.

O QUE É DADO PESSOAL SENSÍVEL?

Os dados pessoais sensíveis têm proteção ainda maior, porque são diretamente relacionados aos aspectos mais íntimos da vida de uma pessoa. Assim, se forem mal utilizados, podem gerar discriminação.

EXEMPLOS dados que revelam origem racial ou étnica • dados que revelam convicção religiosa ou opiniões políticas • dados que revelam filiação a sindicato ou organização de caráter religioso, filosófico ou político • dados genéticos ou biométricos • dados relativos à saúde • dados relativos à vida sexual ou orientação sexual de uma pessoa.

QUEM SÃO AGENTES DE TRATAMENTO?

Os agentes de tratamento são o controlador e o operador. Eles devem manter registro de todas operações de tratamento de dados pessoais que realizam.

CONTROLADOR é a pessoa, natural ou jurídica, que toma as decisões referentes ao tratamento de dados pessoais. Determina as finalidades e os meios de tratamento.

OPERADOR é uma outra pessoa, natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador. Obedece a lei e as ordens do controlador.

O QUE NÃO SÃO DADOS PESSOAIS?

Toda informação que não pode ser associada a uma pessoa específica.

Informação relacionada a uma pessoa jurídica (por exemplo, uma empresa ou uma instituição) não é dado pessoal.

Dado anonimizado também não é dado pessoal. Para entender, um dado anonimizado é um dado que passa por uma técnica que torna inviável identificar a pessoa a quem se refere. Não é possível descobrir de quem é o dado.

QUEM SÃO OS TITULARES?

Titular é a pessoa natural a quem se referem os dados pessoais que são objeto do tratamento. Pela lei, você é o titular dos seus dados pessoais.

QUEM É O ENCARREGADO?

É a pessoa indicada, pelo controlador ou pelo operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Sua função envolve receber reclamações dos titulares, prestar esclarecimentos, adotar providências e orientar os funcionários da instituição sobre a proteção de dados pessoais.

Os principais conceitos no contexto da Defensoria Pública do Estado do Rio Grande do Sul

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

CONTROLADORA
- ARTIGO 15 DA PPDP -

A Defensoria Pública do Estado do Rio Grande do Sul é a controladora dos dados pessoais.

TITULARES DOS DADOS
- ARTIGO 20 DA PPDP -

Toda pessoa natural titular de dados pessoais que sejam tratados pela Defensoria Pública do Estado do Rio Grande do Sul.

EXEMPLOS assistidos • servidores • membros • demais colaboradores.

ENCARREGADO
- ARTIGO 17 DA PPDP -

O encarregado será indicado pelo Defensor Público-Geral do Estado. Deverá possuir conhecimentos essenciais à função, de preferência nas áreas de gestão, privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público.

OPERADORES
- ARTIGO 19 DA PPDP -

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome e por ordem da Defensoria Pública do Estado do Rio Grande do Sul.

EXEMPLOS empresa que fornece serviço de e-mail • empresa que fornece serviço de assinatura eletrônica.

COMPROMISSO DAQUELES QUE TRABALHAM PARA A INSTITUIÇÃO
- ARTIGO 16 DA PPDP -

São deveres de todos os membros, servidores, estagiários e demais colaboradores que executem atividade vinculada à atuação institucional da Defensoria Pública do Estado do Rio Grande do Sul:

- Conhecer e cumprir a Política de Proteção de Dados Pessoais
- Seguir as orientações da controladora
- Observar as leis sobre proteção de dados pessoais, privacidade e medidas de segurança
- Atuar com responsabilidade, critério e ética
- Garantir a segurança da informação
- Comunicar de imediato o encarregado sobre a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa causar dano aos titulares dos dados pessoais

Fundamentos da Lei

ARTIGO 2º DA LGPD

A disciplina da proteção de dados pessoais tem como fundamentos:

Liberdade de expressão, de informação, de comunicação e de opinião

Respeito à privacidade

Desenvolvimento econômico e tecnológico e inovação

Autodeterminação informativa

Livre iniciativa, livre concorrência e defesa do consumidor

Proteção da intimidade, da honra e da imagem

Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania

Aplicação da Lei

ARTIGO 3º DA LGPD

A lei se aplica a toda e qualquer atividade de tratamento de dados realizada, por pessoa natural (exemplo: Fulano de Souza) ou por pessoa jurídica de direito público (exemplo: INSS) ou privado (exemplo: Farmácia Y), independentemente do meio ou da forma, do país de sua sede ou do país onde estejam localizados os dados. Pode ser em formato físico ou digital, em texto, figuras, gráficos, fotografia, vídeo, áudio ou qualquer outro meio possível.

O tratamento também precisa preencher um dos seguintes critérios: (1) deve ser realizado no Brasil; (2) deve ter por objetivo oferecer ou fornecer bens ou serviços ou o tratamento de dados de pessoas localizadas no Brasil; ou (3) deve envolver dados pessoais coletados no Brasil, ou seja, dados pessoais de titulares - brasileiros ou não - que estejam no Brasil no momento da coleta.

Não Aplicação da Lei

ARTIGO 4º DA LGPD

A lei não se aplica ao tratamento de dados pessoais realizado exclusivamente (1) por uma pessoa para fins particulares e sem interesse econômico, (2) para fins jornalísticos, artísticos ou acadêmicos ou (3) para segurança pública, defesa nacional, segurança do estado ou investigações e repressão de crimes. Também não se aplica (4) a dados que vêm de fora do país e que não sejam comunicados ou compartilhados com empresas brasileiras ou então objeto de transferência internacional.

Princípios

ARTIGO 6º DA LGPD

As atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios:

01. FINALIDADE	O tratamento precisa ter finalidades legítimas, específicas, explícitas e informadas de forma clara ao titular.
02. ADEQUAÇÃO	Os dados devem ser tratados de forma compatível com as finalidades informadas ao titular.
03. NECESSIDADE	O tratamento deve se limitar ao mínimo necessário para atingir suas finalidades. Deve envolver apenas os dados essenciais.
04. LIVRE ACESSO	Os titulares podem saber, de modo fácil e gratuito, sobre a forma, a duração do tratamento e quais dados pessoais envolve.
05. QUALIDADE	Os dados devem ser exatos, claros, relevantes e atualizados.
06. TRANSPARÊNCIA	Os titulares devem receber informações claras, corretas e de fácil acesso sobre tudo o que envolve o tratamento.
07. SEGURANÇA	Os dados devem estar seguros. Devem ser protegidos por medidas técnicas e administrativas, evitando acessos não autorizados, destruição, perda, alteração ou até vazamento.
08. PREVENÇÃO	A ocorrência de danos por causa do tratamento de dados pessoais deve ser evitada pelas medidas adequadas.
09. NÃO DISCRIMINAÇÃO	O tratamento não pode ser realizado para finalidades discriminatórias, ilegais ou abusivas.
10. RESPONSABILIZAÇÃO	Quem trata os dados deve demonstrar que adota medidas eficazes e que cumpre as normas de proteção de dados pessoais.

Bases Legais

ARTIGO 7º DA LGPD

O tratamento de dados pessoais somente pode ser realizado nas seguintes hipóteses:

CONSENTIMENTO

Através do fornecimento de consentimento pelo titular.
Exemplo: você baixa um aplicativo, informa seus dados pessoais e clica em aceitar os termos de uso e a política de privacidade.

atenção para a dica 08 da página 22

OBRIGAÇÃO LEGAL

Para o cumprimento de obrigação legal ou regulatória pelo controlador.
Exemplo: para cumprir obrigações trabalhistas e previdenciárias ou determinações da Lei de Acesso à Informação.

POLÍTICA PÚBLICA

Pela administração pública, quando necessário à execução de políticas públicas previstas em leis e regulamentos ou estabelecidas em contratos, convênios ou similares.
Exemplo: fornecimento do auxílio-emergencial ou concessão de passe livre.

PESQUISA POR ÓRGÃO

Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
Exemplo: dados que o IBGE coleta para realizar o censo.

EXECUÇÃO DE CONTRATO

Para a execução de contrato do qual o titular seja parte ou de procedimentos preliminares relacionados ao contrato, a seu pedido.
Exemplo: para cumprir o contrato de fornecimento de telefonia móvel, a empresa precisa de alguns dos seus dados pessoais.

PROCESSO JUDICIAL OU ADMINISTRATIVO

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, não podendo ser utilizados depois em prejuízo do titular.
Exemplo: uso dos dados necessários para cobrar pensão alimentícia em ação judicial.

PROTEÇÃO DA VIDA

Para a proteção da vida ou da incolumidade física do titular ou de terceiro.
Exemplo: uso dos dados de geolocalização do celular de uma pessoa desaparecida.

TUTELA DA SAÚDE

Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
Exemplo: acesso ao prontuário de uma pessoa que necessita de atendimento pelo SUS.

Bases Legais

ARTIGO 7º DA LGPD

INTERESSE LEGÍTIMO

Para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades do titular.
Exemplo: envio de propaganda sobre promoção de um produto para clientes antigos de uma loja de óculos.

PROTEÇÃO AO CRÉDITO

Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
Exemplo: avaliação do score de crédito da pessoa para concessão de um novo empréstimo.

O QUE É O CONSENTIMENTO?

Consentimento é a manifestação de vontade livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Livre, porque o titular pode escolher entre aceitar ou recusar o tratamento. Informado, porque o titular tem a seu dispor informações claras, necessárias e suficientes sobre o tratamento para analisar e formar sua escolha. Inequívoco, porque fornecido por escrito, em cláusula destacada, ou de outra forma evidente e adequada. Logo, não pode ser extraído da omissão, nem de forma implícita, genérica, enganosa ou abusiva.

O consentimento pode ser revogado a qualquer momento através de manifestação expressa do titular, de modo gratuito e facilitado. Caso haja mudanças na finalidade do tratamento ou na forma como é realizado, que não sejam compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre tais alterações, podendo o titular revogar o consentimento, caso não concorde mais.

Não é necessário obter o consentimento para tratar os dados tornados manifestamente públicos pelo titular, desde que preservados os direitos do titular e os princípios em lei.

O QUE É O LEGÍTIMO INTERESSE?

A base legal do legítimo interesse do controlador somente pode fundamentar o tratamento de dados pessoais para finalidades que sejam legítimas, consideradas a partir de situações concretas.

Por exemplo, para o apoio e promoção de atividades do controlador. Ou para a proteção, em relação ao titular, do exercício regular de seus direitos ou para a prestação de serviços que o beneficiem.

Para saber se a finalidade é legítima, pode ser feito um teste de proporcionalidade de 4 etapas, analisando: a legitimidade, a necessidade, o balanceamento e as salvaguardas.

Na sua escolha, o controlador deve sempre respeitar as legítimas expectativas do titular e seus direitos e liberdades fundamentais. Além do mais, deve haver transparência e somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

Bases Legais e a Defensoria Pública do Estado do Rio Grande do Sul

ARTIGOS 7º E 23 DA LGPD

O tratamento de dados pessoais pelas pessoas jurídicas de direito público deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

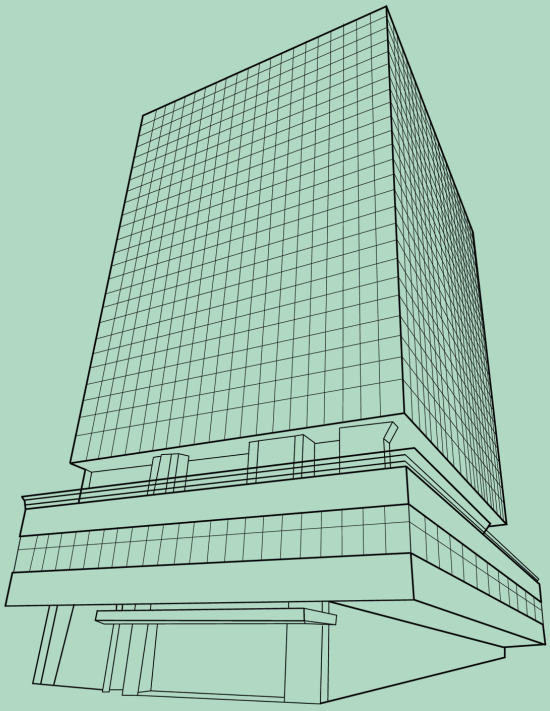
Para tanto, devem ser informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais. Ou seja, devem ser fornecidas informações claras, acessíveis e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.

O mesmo vale para a Defensoria Pública do Estado do Rio Grande do Sul. As regras estabelecidas pela LGPD e pela Política de Proteção de Dados Pessoais devem ser observadas durante todo o ciclo de vida do tratamento de dados pessoais pela instituição, especialmente os princípios gerais e a garantia dos direitos dos titulares.

Além disso, sempre que possível, os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, objetivando a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo público em geral.

O uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.

É importante notar que não há incompatibilidade entre a Lei de Acesso à Informação e a LGPD. No entanto, o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização em um primeiro momento.



conceito está na página 08

Dados Sensíveis

ARTIGO 11 DA LGPD

O tratamento de dados pessoais sensíveis somente pode acontecer (1) quando o titular ou seu responsável legal der consentimento, de forma específica e destacada, para finalidades específicas ou (2) sem o consentimento do titular, nas hipóteses em que for indispensável para:

- Cumprimento de obrigação legal ou regulatória pelo controlador
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
- Realização de estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos
- Cuidado da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
- Proteção da vida ou da integridade física do titular ou de terceiro
- Prevenção à fraude e à segurança do titular nos processos de identificação de cadastro em sistemas eletrônicos, a não ser que no caso de prevaleçam direitos e liberdades fundamentais do titular

Dados de Crianças e Adolescentes

ARTIGO 14 DA LGPD

Criança é a pessoa com até 12 anos de idade incompletos, e adolescente é aquela entre 12 e 18 anos, de acordo com o Estatuto da Criança e do Adolescente. O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado em seu melhor interesse.

Com relação às crianças, o tratamento de dados pessoais deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Esse consentimento é dispensado, no entanto, quando a coleta dos dados for necessária para contatar os pais ou o responsável legal ou para proteger a criança, inclusive mediante o exercício de direitos.

Direitos dos Titulares

CAPÍTULO III DA LGPD

Toda pessoa tem garantidos seus direitos fundamentais de liberdade, de intimidade e de privacidade. Para isso, o titular dos dados pessoais pode exercer os seguintes direitos, de forma gratuita, através de requerimento expresso seu ou de um representante, feito ao controlador:

- confirmar que o tratamento existe
- acessar os dados
- corrigir os dados
- anonimizar, bloquear ou eliminar dados desnecessários ou tratados irregularmente
- portabilidade dos dados a outro fornecedor
- eliminar dados que foram tratados com seu consentimento
- ser informado sobre o compartilhamento de seus dados com terceiros
- se opor ao tratamento irregular
- ser informado sobre a possibilidade de não dar consentimento e quais as consequências
- revogar seu consentimento
- pedir a revisão de decisões tomadas apenas com base em tratamento automatizado
- fazer reclamação ou pedido à ANPD

mais informações na página 21

ARTIGO 20 DA PPDP

Art. 20. [TITULARES E DIREITOS] Toda pessoa natural titular de dados pessoais que sejam tratados pela Defensoria Pública do Estado do Rio Grande do Sul poderá exercer os direitos elencados pelo artigo 18 da Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento e mediante requerimento expresso próprio ou de representante legalmente constituído, por meio de canal de comunicação a ser disponibilizado.

§ 1º Ressalvam-se os casos de impossibilidade jurídica de atendimento da solicitação em virtude de atividade vinculada ao desempenho das atribuições legais da Defensoria Pública do Estado do Rio Grande do Sul, bem como as informações de acesso restrito e as hipóteses justificadas de segredo e sigilo, conforme disposições da Lei de Acesso à Informação e demais normas vigentes.

§ 2º O atendimento às requisições será realizado de forma adequada, observados os princípios da regularidade, continuidade, efetividade, segurança, atualidade, generalidade, transparência e cortesia.

Transparência

ARTIGO 9º DA LGPD

O titular tem o direito de acessar e conhecer as informações sobre o tratamento de seus dados pessoais. Tais informações devem ser disponibilizadas de forma clara pelo controlador, incluindo:

1. finalidade específica do tratamento
2. forma e duração do tratamento
3. identificação e contato do controlador
4. responsabilidades dos agentes que fazem o tratamento
5. direitos do titular
6. informações sobre compartilhamento dos dados

Fim do Tratamento

ARTIGOS 15 E 16 DA LGPD

O tratamento de dados pessoais termina quando:

- A finalidade já foi alcançada
- Os dados já não são necessários ou pertinentes para alcançar a finalidade
- Chegar o fim do período de tratamento
- O titular assim pedir, inclusive no exercício do seu direito de revogar o consentimento, resguardado o interesse público
- A Autoridade Nacional de Proteção de Dados (ANPD) determinar, por ter verificado alguma violação à lei

Depois do fim, os dados pessoais devem ser eliminados, com exceção dos seguintes casos em que podem ainda assim ser conservados:

- Cumprimento de obrigação legal ou regulatória pelo controlador
- Estudo por órgão de pesquisa, devendo ser garantida, sempre que possível, a anonimização dos dados pessoais
- Transferência a uma terceira pessoa, desde que respeitados os requisitos de tratamento de dados da lei
- Uso exclusivo do controlador, desde que proibido seu acesso por terceira pessoa e anonimizados os dados

Boas Práticas

ARTIGO 50 DA LGPD

Os controladores e operadores podem formular regras de boas práticas para o tratamento de dados pessoais, desenvolver soluções de governança de dados e também implementar programa de governança em privacidade. Para isso, podem estabelecer o regime de funcionamento, os procedimentos - incluindo reclamações e pedidos dos titulares -, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de prevenção de riscos.

BOAS PRÁTICAS NA DEFENSORIA PÚBLICA
- ARTIGOS 27 E 28 DA PPDP -

A Defensoria Pública buscará promover, através do seu Centro de Estudos, de Capacitação e de Aperfeiçoamento da Defensoria Pública (CECADEP) ou por meio de parcerias públicas ou privadas, cursos e demais ações de capacitação para garantir que todos conheçam e cumpram o compromisso institucional com a proteção de dados pessoais, a privacidade e as medidas de segurança implementadas, bem como para que desempenhe suas funções de forma eficiente, ética e responsável.

Além disso, as boas práticas adotadas serão divulgadas por campanhas informativas com apoio da Assessoria de Comunicação Social e por meio de conteúdos em linguagem simples e acessível, para promover uma cultura protetiva, com conscientização e sensibilização sobre as questões relacionadas à proteção de dados.

Privacidade por Design e por Padrão

ARTIGO 46, § 2º, DA LGPD + ARTIGO 21, PARÁGRAFO ÚNICO, DA PDPP

A privacidade deve ser protegida desde a fase inicial de criação do produto ou do serviço até a sua execução. Também deve ser protegida por padrão, ou seja, as configurações já garantem a privacidade total, sem que você precise realizar configurações extras para isso.

OS 7 PRINCÍPIOS DA PRIVACIDADE POR DESIGN, por Ann Cavoukian:

1. Proatividade, e não reatividade + prevenção, e não correção • 2. Privacidade como configuração padrão • 3. Privacidade incorporada ao design • 4. Funcionalidade total • 5. Segurança de ponta-a-ponta + proteção total do ciclo de vida • 6. Visibilidade e transparência • 7. Respeito pela privacidade do usuário + centrado no usuário

Segurança

ARTIGOS 46 A 49 DA LGPD

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais. A proteção deve impedir acessos não autorizados e situações - acidentais ou ilícitas - de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilegal.

A obrigação de garantir a segurança da informação é dos agentes de tratamento e de qualquer outra pessoa que intervenha em uma das fases do tratamento, durando mesmo após o seu término.

CONFIDENCIALIDADE	somente pessoas devidamente autorizadas devem ter acesso à informação
INTEGRIDADE	a informação deve manter todas as características originalmente estabelecidas para que seja exata, completa e correta
DISPONIBILIDADE	a informação deve estar acessível e disponível para o uso por parte das pessoas autorizadas

MEDIDAS DE SEGURANÇA NA DEFENSORIA PÚBLICA
- ARTIGOS 21, 22 E 23 DA PPDP -

Na Defensoria Pública, as medidas de segurança, técnicas e administrativas buscam fortalecer o ecossistema de tecnologias da informação e comunicação e observar a legislação do país sobre o tema, tendo por base as normas padrão de referência internacional para a gestão da segurança.

Nesse contexto, toda e qualquer atividade de tratamento de dados pessoais realizada pela Defensoria Pública deve estar em conformidade com essas medidas e ser realizada também em harmonia com a Política de Segurança da Informação e das Comunicações.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA
- ARTIGO 25 DA PPDP -

Se não for tratado de modo rápido e apropriado, um incidente de segurança que envolva dados pessoais pode resultar em graves danos aos titulares, tais como: perda de controle sobre seus dados pessoais, roubo de identidade, dano à reputação, fraude, prejuízos financeiros ou morais, uso indevido de dados sensíveis ou acesso a dados protegidos por sigilo profissional.

É por isso que a ocorrência de qualquer incidente de segurança envolvendo dados pessoais deve ser comunicada imediatamente à equipe responsável e ao encarregado. Em seguida, o controlador deve analisar a situação e, se for o caso, acionar o plano de resposta a incidentes de segurança. O plano contém medidas adequadas - proativas e reativas - capazes de reverter ou mitigar os efeitos do incidente, bem como de tornar os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. Se for verificado que o incidente pode, no caso concreto, causar risco ou dano relevante aos titulares dos dados, devem ser comunicados os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Responsabilidades

ARTIGOS 42 E 44 DA LGPD

O controlador ou o operador que, em razão da atividade de tratamento de dados pessoais, causar a outra pessoa dano patrimonial, moral, individual ou coletivo, violando assim a legislação de proteção de dados pessoais, tem a obrigação de repará-lo.

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

• O modo pelo qual o tratamento é realizado

• O resultado e os riscos que razoavelmente se esperam do tratamento

• As técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado

Também responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança necessárias para proteger os dados pessoais, der causa ao dano.

– ARTIGO 34 DA PPDP –

A inobservância da Política de Proteção de Dados pode ter como consequência a apuração das responsabilidades internas e externas previstas nas normas da Defensoria Pública do Estado do Rio Grande do Sul e na legislação em vigor, podendo caracterizar infração funcional, a ser apurada em processo administrativo disciplinar, ou mesmo haver responsabilização penal, civil e administrativa.

Penalidades

ARTIGO 52 DA LGPD

Os agentes de tratamento de dados que cometerem infrações às normas da LGPD ficam sujeitos às seguintes penalidades administrativas, que podem ser aplicadas pela ANPD:

• Advertência, com prazo para adotar medidas corretivas

• Multa simples, de até 2% do faturamento anual da empresa, chegando ao limite de R$ 50 milhões

• Multa diária, chegando ao limite de R$ 50 milhões

• Divulgação pública da infração, após investigada e confirmada a sua ocorrência

• Bloqueio dos dados pessoais a que se refere a infração, até a sua regularização

• Eliminação dos dados pessoais a que se refere a infração

• Suspensão parcial do funcionamento do banco de dados a que se refere a infração, chegando ao período máximo de 6 meses, prorrogável por mais 6 meses

• Suspensão da atividade de tratamento dos dados pessoais a que se refere a infração, chegando ao período máximo de 6 meses, prorrogável por mais 6 meses

• Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados

Com exceção das multas, todas as penalidades acima podem ser aplicadas às entidades e aos órgãos públicos.

Autoridade Nacional de Proteção de Dados

ARTIGOS 55-A A 55-L DA LGPD

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada pelo Decreto nº 10.474/2020 e é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil.

Clicando aqui você acessa o site oficial e pode conhecer a ANPD, fazer denúncias, solicitações, tirar dúvidas e dar sugestões.

Conforme visto, o titular de dados pessoais possui uma série de direitos, que devem ser atendidos pelo controlador. Em um primeiro momento, os pedidos relacionados aos direitos devem ser realizados diretamente à organização responsável pelo tratamento dos dados. Se o pedido não for atendido, o titular de dados pode então apresentar uma reclamação à ANPD, com a comprovação de que a reclamação não foi solucionada pelo controlador.

Além de várias outras atividades, a ANPD também é responsável por:

- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade
- Fiscalizar e aplicar penalidades quando verificar que o tratamento de dados foi realizado em descumprimento à LGPD, através de um processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso
- Avaliar os pedidos dos titulares contra os controladores, após o titular comprovar que sua reclamação não foi solucionada pelo controlador no prazo estabelecido
- Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança
- Pedir às entidades do poder público que realizem operações de tratamento de dados pessoais, a qualquer momento, que informem o âmbito, a natureza dos dados e os demais detalhes do tratamento, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento da lei
- Decidir, na esfera administrativa, sobre a interpretação da LGPD, as suas competências e os casos omissos

Dicas de Segurança

NO DIA A DIA

01

Cuidado com suas senhas.

Escolha suas senhas cuidadosamente. Faça senhas fortes, que não sejam fáceis de ser desvendadas por terceiros. Não deixe suas senhas anotadas por aí e não repasse a outras pessoas.

02

Tenha critério com o dado que você fornece.

Evite divulgar dados pessoais que não tenham relação nenhuma com o acesso, a contratação ou o ato que você está realizando.

03

Busque se informar.

Procure se informar sobre como seus dados serão utilizados e com quem serão compartilhados. É o caso, por exemplo, da informação do número do CPF na farmácia.

04

Não forneça dados sensíveis a qualquer um.

Não forneça informações sobre sua saúde, religião, convicções políticas, orientação sexual e outras informações de foro íntimo para a realização de qualquer cadastro de loja ou empresa. Seja criterioso e questione a necessidade do dado.

05

Atenção redobrada ao preencher cadastros.

Tenha cuidado ao preencher cadastros na internet para realização de joguinhos, testes de personalidade, mapa astral, aplicativos de envelhecimento, filtros de imagens e outras "brincadeiras" aparentemente inofensivas.

06

Pense antes de fornecer sua impressão digital.

Não permita que coletem sua impressão digital sem real necessidade. É um dado biométrico e sensível. Isso só pode ser feito pelos órgãos oficiais de identificação ou em situações muito restritas.

07

Faça perguntas caso se sinta discriminado.

Questione a empresa se perceber que você está sofrendo algum tipo de discriminação no mercado de consumo. Procure saber por que o preço de um produto ou serviço apresentado a você está mais caro do que o apresentado para outros consumidores.

08

Leia os termos de uso e as pequenas letras.

Leia os termos de uso e as políticas de privacidade das redes sociais e dos aplicativos que você usa. Veja o que vão fazer com seus dados e só dê o consentimento se de fato concordar. Se não concordar, conteste.

09

Mantenha controle de seus aparelhos e logins.

Não deixe seu celular, notebook ou computador ser acessado por pessoas estranhas. Encerre a sessão sempre que sair do e-mail, de redes sociais ou de qualquer aplicativo que exija login.

Dicas obtidas junto ao PROCON/SP e ao SERPRO.
Disponíveis em https://www.procon.sp.gov.br/wp-content/uploads/2020/12/Cartilha-LGPD-2020_11dez.pdf
e em https://www.serpro.gov.br/lgpd/cidadao/voce-ja-protege-seus-dados-pessoais

Dicas de Segurança

NO LOCAL DE TRABALHO

01

Leia a PPDP e coloque o texto em prática.

Leia com atenção a Política de Proteção de Dados Pessoais. Coloque em prática o texto e mantenha uma conduta compatível com as normas de proteção de dados.

02

Cuidado onde você clica.

Não acesse sites desconhecidos e não abra qualquer link de e-mail. Suspeite e, em caso de dúvida, escolha um site mais confiável ou entre em contato com o remetente do e-mail.

03

Garanta a confidencialidade.

Proteja a informação própria da Defensoria Pública e da que lhe é confiada. Respeite a finalidade e não permita a sua divulgação, em especial de dados sigilosos ou pessoais.

04

Mantenha sua mesa e sua tela limpas.

Organize sua mesa e bloqueie sua tela quando não estiver em uso. Garanta que nenhuma informação confidencial ou dados de terceiros serão deixados à vista, seja em papel ou em meio eletrônico.

05

Respeite as senhas e as restrições de acesso.

As informações da Defensoria Pública devem ser acessados apenas pelas pessoas autorizadas para tal. Por isso, não forneça sua senha ou sua chave a quem não deve. Também não aceite usar a senha ou a chave de outra pessoa.

06

Evite conectar pendrives e celulares.

Ao conectar um pendrive ou até mesmo um telefone no computador da Defensoria Pública, você oferece risco elevado devido à facilidade com que vírus e outros programas maliciosos podem se propagar por esses dispositivos.

07

Comunique o incidente de segurança na hora.

Faça comunicação imediata à equipe responsável e ao encarregado quando verificar um incidente de segurança envolvendo os dados pessoais tratados pela Defensoria Pública. Isso pode permitir a adoção de medidas capazes de reverter ou diminuir os efeitos do incidente.

08

Proteja os espaços físicos.

Os espaços físicos - armários, salas ou outros - que contenham informação reservada ou dados pessoais deverão estar fechados e protegidos nos períodos de ausência dos responsáveis por seu cuidado.

09

As regras continuam valendo no trabalho remoto.

Todos os cuidados de segurança devem ser observados no trabalho remoto. Mantenha sempre sob sua vigilância dispositivos móveis ou documentos da Defensoria Pública que estejam em sua guarda.

Leis Relacionadas

Lei nº 8.078/1990
Código de Defesa do Consumidor

Lei nº 9.507/1997
Lei do Habeas Data

Lei nº 12.414/2011
Lei do Cadastro Positivo

Lei nº 12.527/2011
Lei de Acesso à Informação

Lei nº 12.965/2014
Marco Civil da Internet

Lei nº 13.460/2017
Código de Defesa do Usuário do Serviço Público

Para Conhecer Mais

LINKS PARA CURSOS, MATERIAIS E EXTRAS

LEI GERAL DE PROTEÇÃO DE DADOS
Inteiro teor da lei.
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

PORTAL DO GOVERNO FEDERAL
Portal do Governo Federal sobre a LGPD.
https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd

CURSO EV.G - INTRODUÇÃO À LGPD
Curso gratuito elaborado pela Escola Nacional de Administração Pública (Enap) e pelo Instituto Tecnologia e Sociedade (ITS Rio).
https://www.escolavirtual.gov.br/curso/153

CURSO EV.G - LGPD NO SETOR PÚBLICO
Curso gratuito elaborado pela Escola Nacional de Administração Pública (Enap) e pelo Ministério da Economia.
https://www.escolavirtual.gov.br/curso/290

CURSO EV.G - GOVERNANÇA DE DADOS
Curso gratuito elaborado pela Escola Nacional de Administração Pública (Enap) e pelo Ministério da Economia.
https://www.escolavirtual.gov.br/curso/270

CURSO EV.G - DIREITO E NOVAS TECNOLOGIAS
Curso gratuito elaborado pela Escola Nacional de Administração Pública (Enap) e pelo Instituto Tecnologia e Sociedade (ITS Rio).
https://www.escolavirtual.gov.br/curso/323

ITS RIO
Cursos, notícias e publicações sobre tecnologia e privacidade e proteção de dados no país.
https://itsrio.org/

ITS RIO - GUIA LGPD E SETOR PÚBLICO
Guia do ITS Rio sobre LGPD voltado para os órgãos e entidades públicas.
https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf

DATA PRIVACY BRASIL
Cursos, notícias e publicações sobre privacidade e proteção de dados no país.
https://dataprivacy.com.br/

GOVERNO FEDERAL - GUIA DE BOAS PRÁTICAS
Guia do Governo Federal sobre boas práticas da LGPD.
https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd

ID WALL - LGPD COMENTADA
Artigo por artigo da LGPD comentado.
https://guialgpd.com.br/lgpd-comentada/

SERPRO - PORTAL LGPD
Portal da SERPRO com informações, notícias e conteúdos sobre a LGPD.
https://www.serpro.gov.br/lgpd

Contato

DEFENSORIA PÚBLICA DO ESTADO DO RIO GRANDE DO SUL

SITE http://www.defensoria.rs.def.br

INSTAGRAM @defensoriapublicars

TWITTER @_defensoriaRS

FACEBOOK https://www.facebook.com/defensoriars

TELEFONE (51) 3211-2233

ENDEREÇO SEDE
Rua Sete de Setembro
Número 666
Bairro Centro Histórico
Porto Alegre/RS
CEP 90010-190

HORÁRIO DE ATENDIMENTO
de segunda a sexta-feira
das 09 às 12 horas e
das 13 às 18 horas