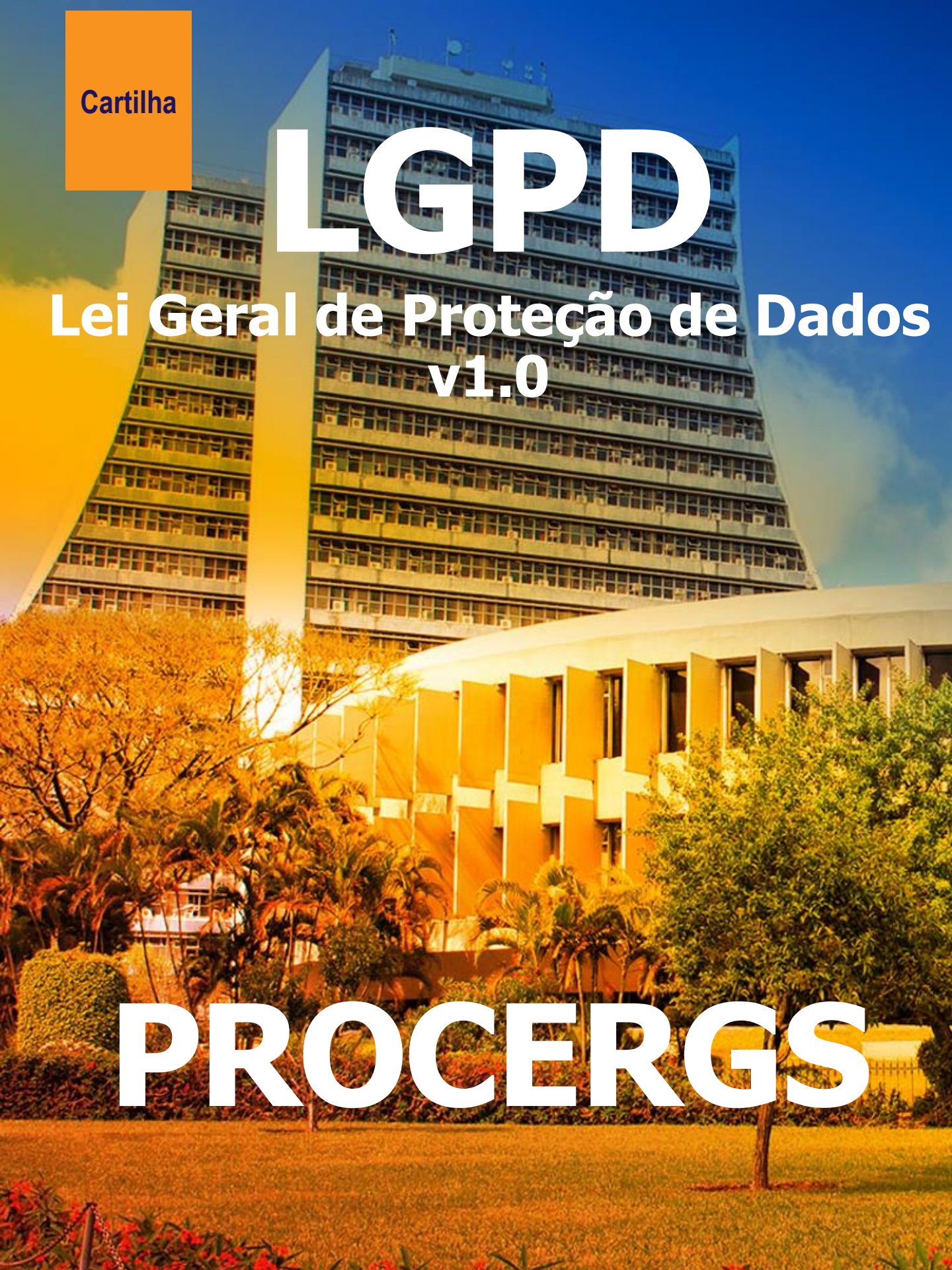
Cartilha

LGPD

Lei Geral de Proteção de Dados

v1.0



PROCERGS

José Antonio Costa Leal

Diretor-Presidente

César Melchior Silveira da Luz

Gerente de *Compliance*

Cristiano Goulart Borges

Encarregado de Dados Pessoais

Cartilha LGPD

Sobre a Cartilha

Cartilha LGPD

OBJETIVOS

1. Objetivos desta Cartilha

1 – Desenvolver a temática da LGPD na PROCERGS de forma simples, clara e didática;

2 – Explorar os conceitos básicos relacionados à LGPD;

3 – Explicar os princípios e as bases legais para tratamento de dados;

4 – Esclarecer os direitos dos titulares de dados;

5 – Esclarecer aspectos da LGPD referentes a Administração Pública;

6 – Fomentar a cultura da Privacidade e da Proteção de Dados na Companhia.

2. O que é a LGPD?

A Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), ou LGPD é um significativo avanço na disciplina de proteção de dados no Brasil.

Embora o Brasil já estivesse se desenvolvendo no que tange a proteção de dados pessoais com legislações setoriais, que abordam essa temática de forma mais fragmentada (Marco Civil da Internet, Código de Defesa do Consumidor, a Constituição Federal de 1988, entre outras), fato é que agora existe uma lei geral, ou seja, se aplica a todo e qualquer setor e está muito mais adequada à realidade digital.

A fundamentação da proteção de dados pessoais trazida pela legislação engloba o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Isso significa dizer que não é objetivo da legislação a total proibição do uso de dados pessoais em qualquer circunstância, mas sim promover o uso desses dados de forma responsável e transparente frente aos seus titulares.

Embora a LGPD tenha entrado em vigor em setembro de 2020, passou a ter vigência plena em agosto de 2021, com a possibilidade de aplicação de sanções administrativas às empresas no caso da não adequação aos preceitos da Lei.

- **Quando se aplica**: quando houver a coleta de dados pessoais de indivíduos localizados no Brasil; quando o tratamento dos dados for realizado no Brasil; ou quando há ofertas de bens e serviços para indivíduos no Brasil.

- **Quando não se aplica**: quando os dados forem provenientes e destinados a outros países, que estejam apenas transitando pelo território nacional; quando o uso dos dados se der no âmbito pessoal e não comercial; para fins jornalísticos, artísticos ou acadêmicos; ou para fins de segurança pública, defesa Nacional, defesa do Estado e atividades de investigação e repressão de infrações penais (os casos de segurança pública e matéria criminal serão objeto de legislação específica, ainda assim, mesmo nesses casos é preciso respeitar os princípios trazidos pela LGPD, bem como os direitos dos titulares).

3. O que muda com a LGPD?

Embora nem todas as questões se enquadrem efetivamente como uma modificação no tratamento, algumas delas são uma mudança de paradigma na coleta e uso dos dados pessoais.

- **Proteção de dados online / off-line**: a LGPD aplica-se tanto ao tratamento digital, quanto analógico, englobando todo e qualquer tipo de documento físico que contenha dados pessoais (planilhas, fichas de funcionários e etc.).

- **Base legal para o tratamento**: dados pessoais (incluindo dados pessoais sensíveis), só podem ser tratados caso se enquadrem numa das hipóteses de tratamento possíveis, especificadas nos art. 7º e 11 da legislação (ver item 6 dessa Cartilha).

- **Princípios da LGPD**: todo e qualquer tratamento de dados pessoais deve respeitar os princípios estipulados pela LGPD. Qualquer tratamento que ignore esses princípios pode configurar-se como uma violação no tratamento de dados pessoais (ver item 5 dessa Cartilha).

- **Direitos dos titulares**: A LGPD, ao especificar uma série de deveres às empresas no tratamento de dados pessoais, sistematiza um catálogo de direitos dos titulares que deverão ser cumpridos e promovidos pelos agentes de tratamento (ver item 7 dessa Cartilha).

- **Adotar medidas de adequação**: a lei exige a implementação de um Programa de Governança em Privacidade que defina, entre outras coisas, norma e boas práticas relativas à proteção de dados, gestão de riscos e salvaguardas adequadas, baseadas num processo de avaliação sistemática de impactos e riscos à privacidade (ver item 10 dessa Cartilha).

- **Fiscalização centralizada**: A Autoridade Nacional de Proteção de Dados – ANPD 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.

4. Conceitos Básicos

Para entender a LGPD é preciso observar conceitos específicos da Lei que se relacionam com a proteção de dados. Como é objetivo da legislação promover transparência numa linguagem simples e de fácil entendimento para os titulares de dados, procurou-se colocar as definições da forma mais clara possível.

- **Dado pessoal**: Na definição da LGPD, o dado pessoal é "toda e qualquer informação relacionada a pessoa natural identificada ou identificável", ou seja, se algo pode te identificar, pode ser considerado um dado pessoal. Essa característica faz com que muitas informações possam ser consideradas dados pessoais. A seguinte lista é exemplificativa e não esgota os possíveis exemplos: nome, endereço, telefone, e-mail, CPF, RG, CNH, Título de Eleitor, Passaporte, Matrícula Profissional, endereço IP, cookies de navegação, momentos de conexão, dados de GPS, números de contas bancárias, número do cartão de crédito, idade, sexo, data de nascimento, local de nascimento, altura, peso, cor do cabelo, cor dos olhos, hábitos (uso de álcool, uso de tabaco, hábitos alimentares) entre outros.

- **Dado pessoal sensível**: Dados pessoais sensíveis, conforme a legislação, tratam-se de dados pessoais 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. Esse tipo de dado "mergulha" na intimidade do titular de dados e usá-los de forma irresponsável pode fazer com que o titular seja vítima de algum tipo de preconceito, atingindo sua dignidade de forma mais profunda e, portanto, precisam de maior proteção.

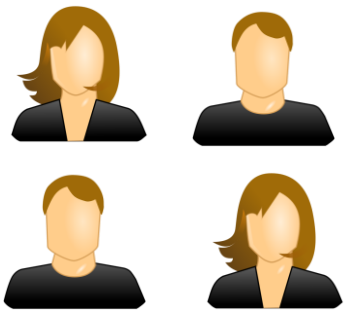
- **Dado anonimizado**: é o tipo de dado que, através da utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, faz com que o dado pessoal perca a possibilidade de associação, direta ou indireta, a um indivíduo. O dado anonimizado perde o caráter de associação à um titular e, portanto, perde justamente a característica que o tornaria um dado pessoal. Aos dados anonimizados, não se aplica a LGPD.

Cartilha LGPD

CONCEITOS

- **Dado pseudoanonimizado**: é o tipo de dado que, através da utilização de meios técnicos, perde a possibilidade de associação, direta ou indireta a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Note-se que o dado pseudoanonimizado permanece com o potencial de identificação do titular, uma vez que basta uma combinação de informações mantidas separadamente para identifica-lo e, portanto, dado pseudononimizado continua sendo dado pessoal.

- **Titular de dados:** o titular é a pessoa natural (ou seja, uma pessoa viva, um ser humano que existe e detém personalidade jurídica), a quem se referem os dados pessoais que são objeto de tratamento.



- **Encarregado de Dados Pessoais**: é a pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O papel do Encarregado é de orientação e adequação, recebendo apoio das áreas responsáveis para adequar a organização à LGPD.

- **Tratamento de dados:** a LGPD define um rol bem extensivo de possibilidades de tratamento de dados pessoais, a saber: 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. Ou seja, praticamente toda e qualquer ação relacionada com o dado pessoal é uma forma de tratamento.

Cartilha LGPD

CONCEITOS

- **Agentes de tratamento**: são considerados os agentes de tratamento o Controlador e o Operador (embora não estejam de forma explícita na lei, existe ainda as figuras do Co-controlador e do Sub-operador que também são agentes de tratamento).

- **Controlador**: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Note que a PROCERGS enquanto pessoa jurídica é considerado o Controlador de dados dos seus empregados. Nem o Presidente da PROCERGS, nem qualquer um dos membros da sua Diretoria, nem qualquer outro empregado da empresa pode ser considerado o Controlador de dados.

- **Operador**: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Note que a PROCERGS, no que se refere aos seus clientes, é um Operador de dados, ou seja, realiza determinados tratamentos de dados pessoais em nome dos seus clientes. Dessa forma, poderíamos dizer que a SEFAZ-RS é um Controlador de dados pessoais e a PROCERGS é um Operador que presta serviços para a SEFAZ-RS. De forma similar ao visto na definição de Controlador, somente a PROCERGS pode assumir a postura de Operador de dados pessoais e não seus empregados, membros da Direção ou Presidência.

5. Princípios

O art. 6º da LGPD define, além da boa fé, uma série de princípios que precisam ser respeitados no tratamento de dados pessoais. Todo e qualquer tratamento de dados pessoais feito pela PROCERGS precisa observá-los. São eles:

- **Princípio da Finalidade**: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Ou seja, todo tratamento de dados precisa ter uma finalidade clara e deve ser transparente ao titular independentemente do seu consentimento. Se há a coleta de um endereço de e-mail para a realização de um serviço, esse dado não pode ser utilizado para outras finalidades.

- **Princípio da Adequação**: "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Ou seja, a empresa deve justificar que os dados coletados tenham valor e sejam condizentes com o modelo de negócio da organização, estando os dados adequados ao tipo de tratamento a ser realizado. Por exemplo, não faz sentido coletar informações de caráter político e religioso para que uma pessoa frequente uma academia de musculação.

- **Princípio da Necessidade**: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Ou seja, apenas os dados indispensáveis para o tratamento devem ser coletados, independentemente da finalidade. Se a coleta de 5 dados pessoais é suficiente para a realização do tratamento não há porque coletar 15 dados pessoais. Lembre-se: não há como estar sujeito a uma violação de dados pessoais que a empresa não possua.

- **Princípio do Livre Acesso**: "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais". Ou seja, o titular é soberano sobre seus dados, podendo solicitar relatórios e informações sobre o tratamento de seus dados ao agente controlador a qualquer momento. Esses mecanismos de consulta devem ser disponibilizados pela empresa de forma gratuita.

- **Princípio da Qualidade dos Dados**: "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento". Ou seja, é preciso garantir que as bases de dados pessoais utilizadas pela empresa sejam fidedignas, atualizadas e alinhadas ao negócio da empresa. Além disso, é garantido ao titular o direito de corrigir informações incorretas, visando sempre manter a qualidade dos dados.

- **Princípio da Transparência**: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Ou seja, as empresas precisam ser honestas com os titulares de dados fornecendo informações claras sobre o tratamento e possíveis compartilhamentos.

- **Princípio da Segurança**: "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Ou seja, é preciso investir em processos, tecnologias e treinamento para garantir a segurança dos dados pessoais, especialmente os dados pessoais sensíveis, para que não ocorram violações no tratamento.

- **Princípio da Prevenção**: "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Ou seja, a velha máxima: "melhor prevenir do que remediar", também se aplica à LGPD. A implementação de medidas de segurança deve ser preventiva e é importante que a empresa esteja preparada para lidar com os problemas caso surjam. O ideal é que haja processos e tecnologias robustas para garantir a proteção dos dados e a privacidade dos titulares.

- **Princípio da Não Discriminação**: "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Ou seja, de forma alguma os dados devem ser tratados para fins discriminatórios ou abusivos, em especial os dados pessoais sensíveis.

- **Princípio da Responsabilização e Prestação de Contas**: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Ou seja, os agentes de tratamento devem comprovar a implementação das medidas de segurança e prevenção, demonstrando-os às autoridades competentes quando necessário. É necessária a geração de evidências de que tais medidas foram efetivamente implementadas.

6 – Hipóteses de Tratamento

A LGPD no seu art. 7º define de forma taxativa as possíveis hipóteses de tratamento de dados pessoais, também conhecidas como bases legais. Da mesma forma, define no seu art. 11 as hipóteses para o tratamento de dados pessoais sensíveis. Para que o tratamento de dados pessoais seja legítimo é preciso que esteja em conformidade com pelo menos uma dessas bases legais.

Todas elas têm o mesmo peso, não existindo uma base que seja mais relevante do que a outra. Note-se que a base legal está atrelada a atividade de tratamento de dados pessoais, ou seja, dentro de uma mesma empresa, até mesmo dentro de um mesmo setor é possível que existam diferentes tipos de tratamento de dados pessoais que podem ser justificados por diferentes hipóteses de tratamento.

Não há uma hipótese de tratamento que se aplique a todas as operações da organização, isso precisa ser observado a cada tratamento de dados individualmente (daí a importância do inventário de dados pessoais). As hipóteses de tratamento definidas pela LGPD são:

- **Para o cumprimento de uma obrigação legal ou regulatória**: Ou seja, quando lidar com dados pessoais for necessário para garantir o cumprimento de outras legislações ou normativas. Um tratamento comum são as obrigações da Companhia relacionadas aos dados de seus empregados. Neste caso as leis trabalhistas não só justificam o tratamento dos dados pessoais como exigem seu armazenamento por longos períodos de tempo. **Exemplo:** Consolidação das leis trabalhistas (art. 168) e Normas Regulamentadoras nº 4 e nº 7: obrigam empresas a realizar exames médicos para comprovar estado de saúde física e psíquica do funcionário.

- **Para a execução de políticas públicas**: Esta base legal é muito específica pois se aplica somente a administração pública e não às empresas em geral (exceto nos casos onde o tratamento ocorre em nome de órgão público na persecução do interesse público). Essa hipótese garante que o Poder Público poderá tratar e fazer uso compartilhado de dados pessoais se eles forem necessários para colocar em prática políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios (não basta afirmar que é uma política pública, é necessário identificar claramente qual política pública embasa o tratamento). **Exemplo:** Tratamento de dados para o Bolsa família (portaria nº 502 de 2017);

Cartilha LGPD

BASES LEGAIS

- **Para a realização de estudos por órgão de pesquisa:** Essa base legitima o tratamento de dados pessoais por órgãos de pesquisa como o IBGE, executando-se, sempre que possível, a anonimização de dados pessoais. Importante ressaltar que não é qualquer tipo de organização que pode utilizar essa base legal para tratamento de dados. De acordo com a Lei, qualifica-se como órgão de pesquisa "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". **Exemplo:** Condução de estudos por instituto de pesquisa públicos como o IBGE a Fiocruz e o IPEA, ou a realização de pesquisa por Universidades Públicas;

- **Para a execução de contrato ou diligências pré-contratuais:** Essa base legitima o tratamento de dados quando forem utilizados para executar ou preparar um contrato no qual o titular seja parte, a pedido do titular. **Exemplo:** Relações de trabalho desde que o uso de dados esteja limitado às suas finalidades;

- **Para o exercício regular de direitos em processo judicial, administrativo ou arbitral**: Essa base legal prevê que os dados pessoais possam ser tratados para exercer direitos em processos judiciais, administrativos ou arbitrais. A arbitragem tem como traços marcantes a intervenção de um terceiro, fora do poder judiciário para a resolução do conflito, o consenso entre as partes (pois a arbitragem somente será aplicável quando houver livre escolha dos envolvidos) e a disponibilidade dos direitos envolvidos. Portanto a LGPD não impede o uso de dados pessoais dentro da legalidade para a produção de provas e defesa em processo, garantindo o direito ao contraditório e a ampla-defesa. **Exemplo:** Apresentação de documentação em juízo: quando o empregador necessita de dados do empregado para comprovar o pagamento de verbas ou concessão de benefícios;

- **Para a proteção da vida ou da incolumidade física do titular ou de terceiro**: Essa base legal garante o uso de dados pessoais caso sejam necessários para proteger a vida do próprio titular de dados ou de terceiros. **Exemplo:** acesso à documentação do titular no caso de ele ter sofrido um acidente e estar impossibilitado de chamar uma ambulância ou de se comunicar com familiares.

Cartilha LGPD

BASES LEGAIS

- **Para a tutela da saúde em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária**: os profissionais de saúde, os serviços de saúde e as autoridades sanitárias estão respaldados pela LGPD para a utilização de dados pessoais que sejam necessários para a realização de suas atividades. **Exemplo:** Tratamento ou procedimento realizado por profissionais de saúde: atendimento médico ou abertura de prontuário.

- **Para a proteção ao crédito**: essa base legal garante o uso de dados pessoais pelos órgãos de proteção ao crédito, de forma que possam continuar incluindo dados de consumidores (titulares) em cadastros positivos, e para que as empresas as quais o titular tenha pendências financeiras possam comunicar essa dívida aos órgãos competentes. Assim, o mercado pode continuar consultando os órgãos de proteção ao crédito para avaliar o perfil do pagador. **Exemplo:** Avaliação de crédito por instituição financeira para que possa oferecer ao titular crédito pré-aprovado de cheque-especial.

- **Para atender um legítimo interesse do controlador**: essa base legal é de uso genérico, entretanto requer absoluto cuidado por parte do Controlador. De acordo com a LGPD, dados pessoais podem ser tratados quando forem necessários para atender aos interesses legítimos do controlador ou de terceiro, desde que esse tratamento não se sobreponha aos direitos e liberdades fundamentais do titular e que seja realizado para finalidades legítimas, consideradas a partir de situações concretas. Note-se que essa base legal não pode ser utilizada para o tratamento de dados pessoais sensíveis e, de forma geral, traz mais responsabilidades para a empresa que a qualquer momento deve estar pronta para justificar o uso desses dados (a ANPD poderá solicitar ao controlador um Relatório de Impacto à Proteção de Dados Pessoais, quando o tratamento estiver baseado no legítimo interesse). Importante ressaltar que, embora a LGPD não explicite na sua redação, é importante que se aplique um teste de ponderação chamado LIA (*Legitimate Interests Assessment*) que atestará o alinhamento do tratamento ao princípio da responsabilidade, previsto na legislação. **Exemplo:** análises comportamentais de clientes para oferecer melhores recomendações de acordo com o interesse do titular (Netflix).

- **Mediante o consentimento do titular de dados**: uma das bases mais conhecidas da LGPD, o consentimento garante que o tratamento de dados pessoais seja realizado para finalidades específicas, mediante a autorização (consentimento) do titular de dados. Embora seja uma das bases mais comentadas da LGPD, não é uma base hierarquicamente prioritária em relação as demais. É preciso atentar-se que, para que o consentimento seja válido, algumas premissas devem ser respeitadas:

1 – O consentimento precisa ser uma manifestação livre, uma escolha real do titular, sobre a qual ele realmente tem controle. Se assim não o for, se o titular sentir-se obrigado a consentir ou vier a sofrer consequências negativas pelo não consentimento, então esse consentimento não é válido.

2 – O consentimento precisa ser informado: o titular deve receber informações suficientes que lhe capacitem para tomar uma decisão consciente de forma clara, sem ambiguidades e sem o costumeiro "juridiquês" utilizado em relações contratuais.

3 – O consentimento precisa ser inequívoco: o consentimento deve manifestar uma ação afirmativa por parte do titular, ou seja, ele deve realizar uma ação deliberada que consinta com o tratamento dos seus dados. Exibir um check box com todas as opções já marcadas, restando apenas ao titular clicar em aceito não representa uma manifestação afirmativa. Da mesma forma, o aceite tácito ("ao continuar com o uso desse serviço, você aceita...", ou seja, o silêncio e a inatividade por parte do titular), também não é uma expressão válida de consentimento. **Exemplo:** Formulário de envio de Newsletter ou a utilização de dados dos empregados para fins diversos e não previstos em contrato: aniversários em murais, tempo de casa e etc.

Cartilha LGPD

BASES LEGAIS

As hipóteses de tratamento relacionadas (especificadas no art. 7º) dizem respeito ao tratamento de dados pessoais? E quanto aos dados pessoais sensíveis?

Quando se fala em dados pessoais sensíveis as hipóteses de tratamento estão definidas no art. 11 e são mais restritivas sendo que o consentimento é a regra. Entretanto não há a necessidade de obter o consentimento quando o tratamento for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador (hipótese também prevista no art. 7º);

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (hipótese também prevista no art. 7º);

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (hipótese também prevista no art. 7º);

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (hipótese também prevista no art. 7º);

e) proteção da vida ou da incolumidade física do titular ou de terceiro (hipótese também prevista no art. 7º);

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (hipótese também prevista no art. 7º);

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (hipótese nova, exclusiva para o tratamento de dados pessoais sensíveis, que não estava prevista no art. 7º).

Note que não se admite a utilização das hipóteses do "Legítimo Interesse do Controlador" ou da "Proteção ao Crédito" para justificar o tratamento de dados pessoais sensíveis.

7. Direitos dos Titulares

O titular de dados pessoais tem alguns direitos garantidos pela LGPD, podendo obter junto ao agente Controlador, a qualquer momento e mediante requisição:

- A confirmação da existência do tratamento;

- O acesso aos dados tratados;

- A correção de dados incompletos, inexatos ou desatualizados;

- A anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;

- A portabilidade dos dados para outro fornecedor de serviço ou produto;

- A eliminação de dados pessoais tratados sob a hipótese do consentimento do titular;

- A informação sobre com quais entidades, públicas e privadas, seus dados foram compartilhados;

- Ser informado sobre a possibilidade de não fornecer seu consentimento e as consequências da negativa;

- Revogação do consentimento, nas hipóteses em que essa base legal tenha fundamentado o tratamento;

- Peticionar em relação aos seus dados pessoais contra o Controlador, perante a ANPD;

- Opor-se ao tratamento realizado numa das hipóteses de dispensa de consentimento, caso o tratamento esteja em desconformidade com a lei.

8. Dados com ciclo de vida?

Sim, os dados têm um ciclo de vida a ser respeitado dentro das organizações!

A LGPD inaugura uma nova visão no tratamento de dados pessoais. Antigamente era muito comum coletar-se o máximo possível de dados pessoais e depois utilizá-los quando fossem, um dia, necessários. Com a LGPD o mínimo de dados para atingir a finalidade especificada deve ser coletado e, a priori, eles não devem ser tratados eternamente. O ciclo de vida dos dados deve ser identificado na etapa de mapeamento e deve-se inclusive identificar em quais etapas há a atuação de um agente Operador. As etapas são:

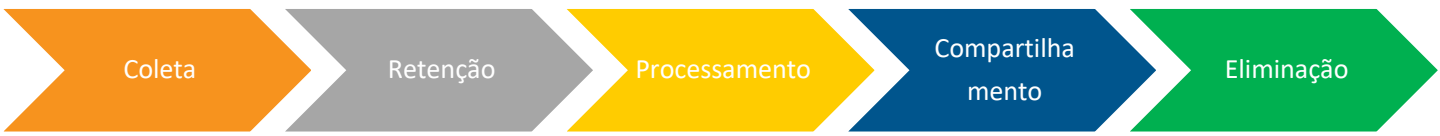
- **Coleta**: Obtenção, recepção ou produção de dados pessoais, independentemente do meio utilizado (documento físico, eletrônico, sistema de informação e etc.).

- **Retenção**: Arquivamento ou armazenamento de dados pessoais independentemente do meio utilizado (documento físico, eletrônico, banco de dados, arquivo de aço, e etc.);

- **Processamento**: Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais;

- **Compartilhamento**: Qualquer operação que envolva reprodução, transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais;

- **Eliminação**: Qualquer operação que vise apagar ou eliminar dados pessoais. Contempla o descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.



9. LGPD e a Administração Pública

O Poder Público através de seus órgãos, diferentemente das empresas privadas, administra as maiores bases de dados com informações dos cidadãos. Um titular de dados pode escolher não se relacionar com uma determinada empresa, entretanto, inevitavelmente e, em algum nível, ele se relacionará com o Poder Público, do seu nascimento até o fim da sua existência. Essa relação é tão significativa que a LGPD dedicou um capítulo inteiro sobre o tema compreendido entre os arts. 23 e 30.

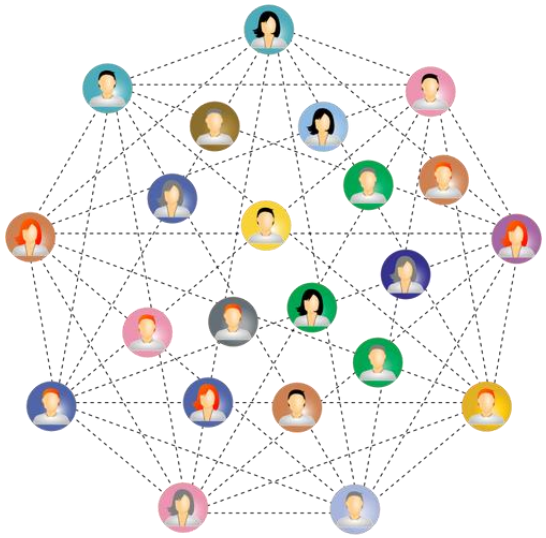
O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

A LGPD utiliza a definição de "pessoas jurídicas de direito público" da Lei de Acesso à Informação e compreende:

- os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

- as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

- Note-se que as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, entretanto, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.



9. LGPD e a Administração Pública

Um ponto de atenção importante é que a Lei veda aos órgãos públicos transferir dados pessoais das bases de dados as quais tem acesso para entidades privadas exceto em casos específicos como:

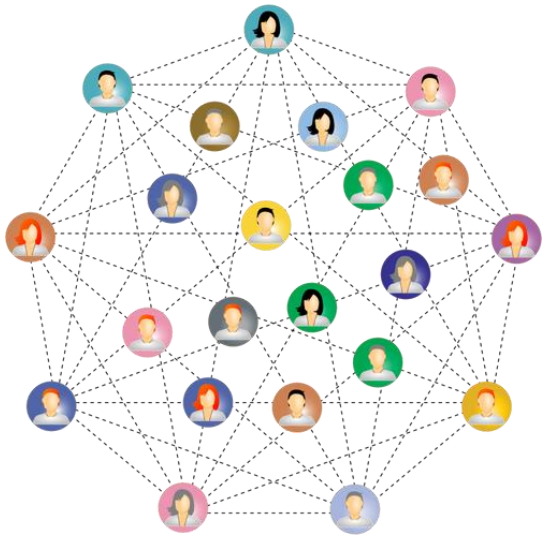
- em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

- nos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD;

- quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres. Estes contratos e convênios deverão ser comunicados à autoridade nacional; ou

- na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Outro ponto de atenção diz respeito à transparência no tratamento dos dados pessoais, não apenas pelo Poder Público, mas especialmente por ele. Como vimos anteriormente, um dos princípios para o tratamento dos dados é a transparência e deve-se sempre levar em consideração que a exceção do consentimento não significa dizer que o Poder Público não deva ser transparente nas suas ações.



10. Programa de Governança

No seu capítulo de Segurança e Boas Práticas a legislação de proteção de dados especifica a implantação de um Programa de Governança em Privacidade (PGP) que:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

10. Programa de Governança

Percebe-se, portanto, que o PGP não se trata de um projeto com início, meio e fim e sim uma jornada que se inicia. O PGP da PROCERGS define ciclos de preparação, execução e monitoramento das diversas atividades necessárias para adequação e que visam promover maior responsabilidade no uso de dados pessoais e garantir a conformidade da empresa à legislação. De forma resumida o PGP da PROCERGS estrutura-se da seguinte forma:

11. Sobre as Sanções

A LGPD prevê determinadas sanções administrativas que serão aplicadas pela Autoridade Nacional de Proteção de Dados. As sanções estão definidas no art. 52º e compreendem:

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

- 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;

- multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

- publicização da infração após devidamente apurada 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 pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Note-se que, no mesmo artigo estão definidos os parâmetros e critérios para a aplicação das sanções que levará em consideração a gravidade e natureza da infração, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência da violação, o grau do dano causado pela violação, a cooperação do infrator, a adoção reiterada e demonstrada pelo infrator de mecanismos e procedimentos internos capazes de minimizar o dano, a adoção de políticas de boas práticas e governança pelo infrator, a pronta adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Cartilha P.&P.D.

CONTATO

Tem dúvidas sobre essa cartilha? Entre em contato.

Encarregado de Proteção de Dados Pessoais

Cristiano G. Borges

e-mail: encarregado-dados@procergs.rs.gov.br

PROCERGS
SOLUÇÕES QUE TRANSFORMAM
50 ANOS

GOVERNO DO ESTADO
RIO GRANDE DO SUL
SECRETARIA DE PLANEJAMENTO, GOVERNANÇA E GESTÃO

13. Referências

- BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso a Informação**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 04 maio 2022.

- BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais** (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm>. Acesso em: 04 maio 2022.

- BRASIL. **Segurança e Proteção de Dados. Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais** (LGPD). Disponível em: <https://www.gov.br/ governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd>. Acesso em: 04 maio 2022.

- ENAP – ESCOLA NACIONAL DE ADMINISTAÇÃO PÚBLICA. **Proteção de Dados Pessoais no Setor Público**. Disponível em: <https://www.escolavirtual.gov.br/ curso/290>. Acesso em: 04 maio 2022.

- GET PRIVACY. **10 bases legais da LGPD que justificam o tratamento de dados: consentimento, legítimo interesse e mais**. Disponível em: < https://getprivacy.com.br/entenda-as-bases-legais-da-lgpd/>. Acesso em: 04 maio 2022.