CARTILHA ORIENTATIVA

LGPD
e o Impacto nas Prefeituras

SECRETARIA DE TRANSPARÊNCIA
E CONTROLADORIA

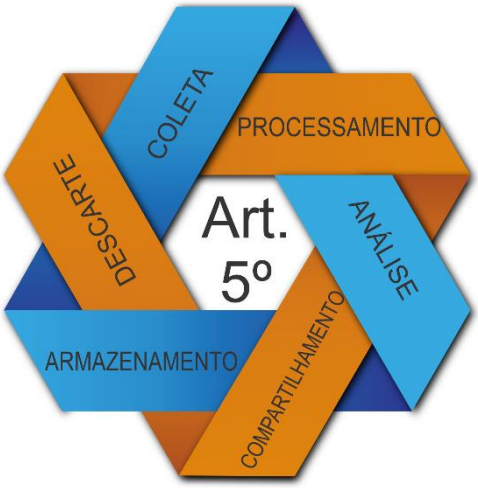
porto alegre
PREFEITURA
Mais **cidade**. Mais **vida**.

APLICAÇÃO DA LGPD NAS PREFEITURAS

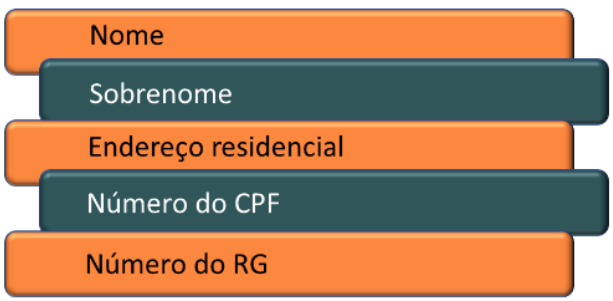
Temos visto, cada vez mais, que a tecnologia está muito presente na vida de todos, não sendo diferente no poder público, mais precisamente nas prefeituras, onde temos visto várias inovações, tais como utilização de drones, sistemas de monitoramento eletrônico, big data etc. Com isso, a coleta/utilização de dados e troca de informações acompanha este crescimento exponencial da tecnologia. As prefeituras possuem uma série de informações que são geradas e tratadas e, dentre elas, dados pessoais, sejam de estudantes, usuários do sistema de saúde, fornecedores, colaboradores, contribuintes, dentre outros.

Diante deste cenário e, visando garantir o direito fundamental à privacidade e a equiparação com o cenário internacional, viu-se a necessidade de uma regulação que vise à tutela da proteção de dados pessoais. Desta forma, em 14 de agosto de 2018, foi sancionada a Lei 13.709, também conhecida como LGPD (Lei Geral de Proteção de Dados Pessoais), a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

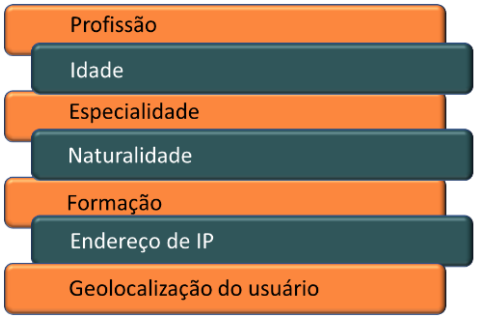
A Lei regula as atividades e o tratamento dos dados entre empresas, instituições de terceiro setor ou organizações religiosas, órgãos públicos e pessoas físicas. Desta forma, temos que entender o que é tratamento de dados pessoais. Pois bem, tratamento é qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados. A mera visualização de dados por um servidor público já caracteriza tratamento, estando, assim, sob o escopo da LGPD. Lembrando que a LGPD só se aplica aos dados pessoais, que são aqueles relacionados à pessoa natural (física) identificada ou identificável. Na ilustração ao lado podemos entender o ciclo de vida dos dados.



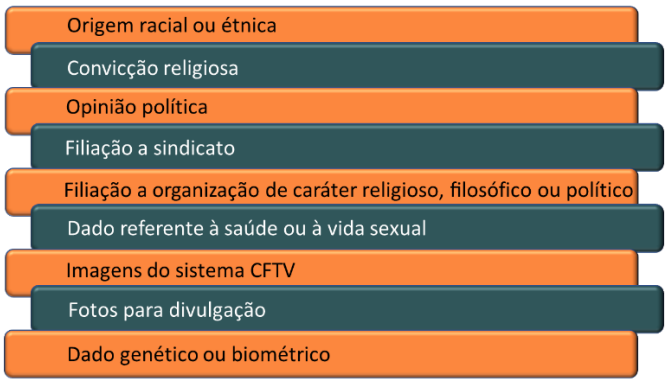
Os dados pessoais identificados se referem a qualquer informação que possa individualizar seu titular, sendo relacionado a uma pessoa específica, como no seguinte exemplo:



Além destes dados identificados, também é do escopo da LGPD os dados pessoais identificáveis: são aqueles que, quando analisados conjuntamente com outras características, possibilitam a identificação de uma pessoa através de referências como, por exemplo:



Existem, ainda, os **dados pessoais sensíveis**, que são aqueles que, devido à sua sensibilidade, podem levar a atitudes discriminatórias contra seus titulares e, por esse motivo, precisam de proteção especial. São exemplos:



Importante esclarecer que a LGPD não veio para proibir o uso dos dados pelas empresas, mas sim para regrar o seu uso, trazendo 10 hipóteses que garantem a legalidade no tratamento dos dados e auxiliam na criação de uma relação mais justa com o consumidor. A mais comum é o consentimento, que é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, ou seja, ele deverá ser claramente informado dos termos de uso e extensão da autorização e precisa concedê-lo livremente. Mas esta não é a hipótese de tratamento que legitima o uso dos dados, pois, em que pese seja a mais difundida, temos mais 9, as quais estão apresentadas na imagem a seguir:

Importante registrar que nenhuma destas hipóteses, ou bases legais, é superior ou preferencial a outra e não possuem dependência ou predominância entre si.

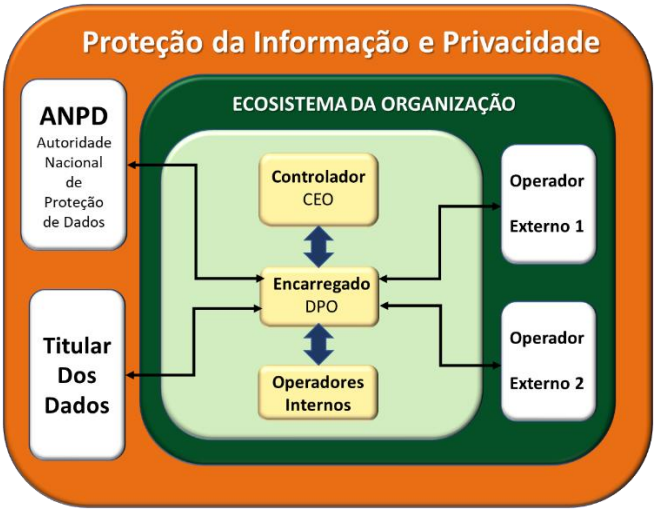
Além destas bases legais, a LGPD traz alguns princípios que norteiam esta norma, os quais visam garantir a transparência no uso dos dados, onde as empresas devem informar a finalidade de uso dos dados, a adequação a esta finalidade, a necessidade de uso destes dados, dentre outros, além de garantir que estes dados estão seguros contra ameaças e riscos à proteção e privacidade de dados.

Mas, afinal, a LGPD foi pensada para proteger os direitos do cidadão, direito este já garantido pela Constituição Federal de 1988, mais precisamente pelo Art. 5º, inciso X, que trata do direito à privacidade, sendo um direito humano fundamental, conforme trata a Declaração Universal dos Direitos Humanos de 1948, reforçado pela Emenda Constitucional 115/2022, a qual torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental. Então, em sendo uma lei focada no cidadão, onde este se beneficia com ela? Pois bem, antes mesmo do advento da LGPD, o cenário que já se apresentava dava conta de que cada vez mais pessoas estão se colocando na condição de titulares dos dados e percebendo que existe uma legislação que protege os seus interesses. Em consequência, a tendência é um aumento de questionamentos judiciais desses titulares perante as empresas, buscando reparação a danos.

O importante é que a LGPD, ao empoderar os cidadãos, dá a ele controle sobre seus dados e a possibilidade de punir os responsáveis por qualquer dano causado pelo mau uso das suas informações. Para isso, a lei garante 9 direitos aos titulares de dados pessoais, os quais serão abordados na sequência desta cartilha.

Já vimos que a lei vale para todos, então, como as prefeituras devem se adequar a ela?

Pois bem, primeiramente temos que entender alguns conceitos e princípios dessa lei, para que possamos saber por onde começar. A LGPD nos traz uma estrutura de governança que apresenta algumas figuras definidas que vamos apresentar aqui. Na imagem abaixo, temos uma estrutura gráfica que ilustra melhor os principais envolvidos nesta legislação.



A seguir, descrevemos melhor cada um destes elementos:

TITULAR DOS DADOS: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento nos processos da organização, pelo fato de que, de alguma forma estão relacionadas com as atividades legítimas.

CONTROLADOR: No âmbito interno, o controlador é o representante legal da organização, normalmente o presidente (CEO), que é o responsável por ela, que por meio dos seus poderes e atribuições delega as ações necessárias para operacionalizar a Política da Proteção de Dados Pessoais e Privacidade dentro da estrutura. Para o ambiente externo, o Controlador é a própria organização que exigirá das pessoas físicas e das pessoas jurídicas, de Direito Público ou Privado, com quem se relaciona, o cumprimento dessa política quando aquelas estiverem tratando dados pessoais originários da Organização.

ENCARREGADO DE DADOS: Pessoa natural, indicado pelo controlador, cujas atribuições estão definidas nos incisos do Parágrafo 2º do Art. 41 da LGPD que são:

I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II. receber comunicações da autoridade nacional e adotar providências;
III. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Todas as prefeituras precisarão de um DPO, porém, este pode ser terceirizado, o que reduz custos e garante a independência e conhecimento necessários ao mesmo.

OPERADORES INTERNOS: São todos os colaboradores que, na execução das atividades relativas aos processos da organização, têm contato e tratam dados de pessoas naturais.

OPERADORES EXTERNOS: São as organizações que compõe o Ecossistema da Proteção de Dados da organização que, para cumprir legislações e atividades específicas relacionadas com as finalidades, tratam dados dos titulares a ela vinculados. Por exemplo, um

escritório que preste serviços jurídicos ou contábeis para a organização, e acessam dados pessoais controlados por ela, são operadores externos.

ANPD: Autoridade Nacional de Proteção de Dados (ANPD) – Órgão da administração pública que é responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Além de regulamentar as diretrizes que as empresas devem seguir ao lidar com dados pessoais, a Lei Geral de Proteção de Dados também assegura os direitos dos titulares de dados, os quais devem ser atendidos pelas pessoas jurídicas ou físicas que tratam dados pessoais com fins comerciais. Para um processo de adequação à lei, é fundamental conhecer o que, exatamente, a LGPD elenca como sendo esses direitos, que estão expressos no Art. 18 da lei.

Ainda, a LGPD deixa claro, em seu Art. 17 que os dados pertencem ao indivíduo, e não à empresa/ instituição que controla ou opera esses dados.

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

Sendo assim, ficam expressos os direitos do titular de dados, conforme seguem:

1. **Confirmação da existência de tratamento**: segundo a LGPD, o titular dos dados tem o direito de confirmar se uma empresa realiza o tratamento de seus dados pessoais. A LGPD estabelece ainda que a resposta pode ser feita de forma imediata e de maneira simplificada, ou por meio de declaração "clara e completa", que indique a origem dos dados, os critérios usados e a finalidade do tratamento. O prazo para a resposta no formato completo é de até 15 dias contado a partir da data do requerimento, conforme estabelece o Art. 19.

2. **Acesso aos dados**: além de saber se a empresa trata seus dados pessoais, o titular também pode pedir acesso aos dados. Ou seja, é possível obter uma cópia dos dados pessoais que a empresa possui em seus arquivos.

3. **Correção de dados**: outro direito do titular de dados é solicitar à empresa a correção de dados pessoais incompletos, inexatos ou desatualizados.

4. **Anonimização, bloqueio ou eliminação de dados**: caso queira, o titular de dados também tem o direito de solicitar a anonimização (processo que torna um dado impossível de ser vinculado a um indivíduo), bloqueio ou eliminação de dados quando eles forem "desnecessários, excessivos ou tratados em desconformidade" com a lei. Por exemplo, se a empresa trata dados que não são necessários para alcançar a finalidade do tratamento ou se o tratamento não é enquadrado em nenhuma das bases legais previstas na lei.

5. **Portabilidade dos dados**: por este direito o titular de dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de serviço ou produto.

6. **Eliminação dos dados tratados com consentimento**: nos casos em que o titular dos dados consentiu com o tratamento, mas mudou de ideia e não quer mais que a empresa trate seus dados pessoais, ele pode solicitar a eliminação desses dados. No entanto, há situações em que esse direito não pode ser exercido, como quando a empresa precisa conservar os dados para cumprir obrigação legal ou regulatória.

7. **Informações sobre o compartilhamento de dados**: considerando que um dos princípios da LGPD é a transparência, é direito do titular saber exatamente com quem o controlador está compartilhando seus dados.

8. **Informação sobre a possibilidade de não fornecer consentimento**: a premissa do consentimento é que ele seja pedido e concedido de forma clara, transparente e totalmente livre. Para isso, o titular de dados tem o direito de ser informado sobre a possibilidade de não fornecer o consentimento e de quais as consequências caso o consentimento seja negado.

9. **Revogação do consentimento**: segundo apregoa a LGPD, qualquer consentimento dado para o tratamento de dados pessoais pode ser revogado. Este é um direito do titular de dados, que pode fazer uma solicitação revogando o consentimento, o que é diferente da eliminação de dados, tratada anteriormente.

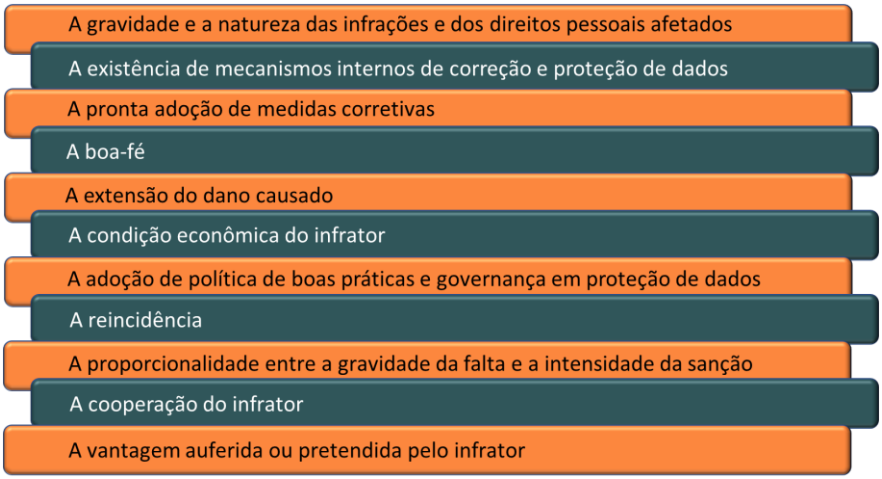
POR QUE AS PREFEITURAS DEVEM SE ADEQUAR À LGPD?

São vários os impactos para quem não cumprir com a LGPD, e devem ser divididos em duas instâncias, a judicial e a administrativa. Na judicial, os titulares de dados, desde o início da vigência da lei, já podem judicializar as situações de descumprimento, sendo que, já temos pequenas, médias e grandes empresas condenadas. A indústria das ações indenizatórias com base na LGPD já iniciou e devemos estar atentos a isso.

Quanto à esfera administrativa, esta se iniciou em 1º de agosto de 2021, em função da lei 14.010/2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Esta lei determinou, em seu artigo 20 que os artigos 52, 53 e 54 da lei 13709/2018 passariam a valer a partir do dia 1º de agosto de 2021.

A Autoridade Nacional de Proteção de Dados (ANPD), conforme já falamos, é o grau hierárquico máximo da Lei Geral de Proteção de Dados. A ANPD é responsável por fiscalizar o tratamento de dados em todo o território nacional e aplicar as correções e sanções pertinentes, caso a lei seja desobedecida. São várias as penalidades que podem ser aplicadas pela ANPD. Discriminadas no artigo 52 da LGPD, elas variam entre aplicação de advertências, com indicação de prazo para adoção de medidas corretivas, multas, ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados. As multas, por sua vez, vão de 2% (dois por cento) do faturamento da empresa no último exercício com teto máximo de R$ 50.000.000,00 (cinquenta milhões de reais) por infração, existindo, ainda, a possibilidade de incidência de multa diária para compelir a entidade a cessar as violações. De toda forma, a aplicação de qualquer dessas penalidades pode ter impacto bastante negativo sobre a atividade empresarial, não somente no aspecto financeiro, mas também no reputacional e operacional.

Para a correta mensuração e aplicação das sanções, a ANPD deverá considerar os seguintes parâmetros:



Importante nos atentarmos que a lei prevê uma responsabilidade solidária entre o controlador e o operador, descrita no artigo 42 da LGPD, sendo assim, temos que ter um rigoroso acompanhamento dos fornecedores e parceiros com quem a prefeitura se relaciona, pois, se estes não estiverem adequados e os contratos não tiverem cláusulas de proteção e privacidade de dados, qualquer incidente com dados pessoais atingirá a prefeitura, que responderá solidariamente.

Cumpre reforçar, que tais sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados não excluem as penalidades civis decorrentes do não tratamento correto dos dados, como os previstos na Lei de Improbidade Administrativa – LIA (Lei nº 8.429/1992) ou Lei de Acesso à Informação – LAI (Lei nº 12.527/2011).

A LAI, por exemplo, em seu artigo 34 já prescreve que os "órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais". A LIA define como ato de improbidade atentatório aos princípios da administração pública qualquer ação ou omissão que viole o princípio da legalidade, por exemplo. Ou seja, não cumprir uma determinação legal pode constituir ato de improbidade administrativa, e como tal, sujeita as seguintes sanções: "ressarcimento integral do dano, se houver, perda da função pública, suspensão dos direitos políticos de três a cinco anos, pagamento de multa civil de até cem vezes o valor da remuneração percebida pelo agente e proibição de contratar com o Poder Público ou receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, ainda que por intermédio de pessoa jurídica da qual seja sócio majoritário, pelo prazo de três anos" (artigo 12, III da Lei nº 8.429/1992).

O próprio Conselho Nacional de Justiça, através da recomendação nº 89 de fevereiro de 2021 recomendou "aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD."

Além do mau ou não tratamento adequado dos dados dos cidadãos, existe, ainda, a possibilidade de condenação em razão da falta de investimentos em cibersegurança. Isso porque o artigo 44 da LGPD expressamente menciona que o tratamento é considerado irregular quando deixa de observar a legislação ou quando não fornece a segurança que o titular dele

pode esperar. E não tem sido incomum a ocorrência de ciber-ataques a diversos sítios de órgãos públicos.

LGPD NO PODER PÚBLICO

O capítulo IV da lei versa sobre o TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. O Art. 23 da LGPD define que 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. Conforme o art. 1º, § 1º da Lei 12.527/2011, são entes do poder público:

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

II - 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.

Sendo assim, as prefeituras municipais estão enquadradas neste ordenamento e deverão atender o que preconiza o capítulo IV da LGPD.

CONDIÇÕES PARA O TRATAMENTO DOS DADOS PELO PODER PÚBLICO:

- sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
- seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, que deve ser pessoa física, seja agente do órgão ou entidade, seja terceirizado.

USO COMPARTILHADO PELO PODER PÚBLICO:

- Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
- O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

COMPARTILHAMENTO COM ENTIDADES PRIVADAS:

- Via de regra vedado.
- Nos casos excepcionais deve ser comunicado à ANPD.

- Exceções:
    - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado;
    - nos casos em que os dados forem acessíveis publicamente;
    - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;
    - 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.

SEGURANÇA E SIGILO DE DADOS

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

Baseado nos princípios da Segurança e da Prevenção, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá implementar Programa de Governança em Privacidade.

O Programa de Governança em Privacidade deve:

a) demonstrar 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) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) contar com planos de resposta a incidentes e remediação; e
h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Para que a organização evite alguma penalização em função da LGPD é necessário que passe por um projeto de adequação, devendo seguir, no mínimo, os seguintes passos:

1. Analisar de que Forma a organização é impactada pela LGPD:

(i) Como, por que, e quais categorias de dados pessoais são tratadas pela organização;

(ii) Analisar o ciclo de tratamento de dados pessoais, desde a coleta até o descarte, identificando a finalidade da utilização.

2. Analisar e documentar as bases legais para o tratamento de dados, para aqueles submetidos à LGPD.
3. Obter os consentimentos necessários, se for o caso.
4. Revisar e detalhar a política de privacidade, tornando públicos os seus termos aos interessados.
5. Definir e documentar as bases legais das transferências internacionais de dados, se for o caso.
6. Adaptar os canais de comunicação e a política e os processos internos destinados a atender os direitos dos titulares.
7. Designar o encarregado de proteção de dados.
8. Revisar os acordos e contratos da organização impactados pela LGPD.
9. Desenhar e implementar as medidas necessárias para garantir a segurança dos dados.
10. Implementar políticas e procedimentos para lidar com a ocorrência de eventuais incidentes.
11. Identificar os possíveis riscos no tratamento de dados, de modo que as medidas necessárias para reduzi-los sejam identificadas e implementadas.

DOCUMENTOS NECESSÁRIOS PARA SE ADEQUAR À LGPD (*disclaimers*)

1) Política de Privacidade e Proteção de Dados:

A política de privacidade ("PP") é um documento que explica como os dados pessoais são tratados. Ela é essencial para qualquer organização. A PP visa atender o princípio da transparência da LGPD.

A política de privacidade precisa conter, no mínimo:

- Quais dados serão tratados
- A finalidade para qual serão tratados
- Por quanto tempo os dados serão retidos
- Com quem os dados serão compartilhados

2) Termos de Uso

Esse documento informa ao usuário quais Termos e Políticas são aplicáveis ao serviço prestado. Além disso, alerta que, ao utilizar o serviço, o usuário concorda expressamente com os termos dele.

Conceitos importantes, como termos técnicos ou legais, precisam ser explicados para melhor entendimento. É fundamental que a forma de linguagem utilizada para esclarecer os significados das palavras seja simples e compreensível, evitando o uso de siglas, jargões e estrangeirismos .

O Termo de Uso deve evidenciar de forma clara quais são as responsabilidades de cada parte envolvida no serviço. Ao definir responsabilidades, a Administração Pública e o cidadão estabelecem direitos e deveres para ambas as partes e compreendem suas obrigações ao utilizar e prover o serviço, de forma a esclarecer quais situações configuram violações aos Termos e para quais situações cabem reparação de danos.

Recomenda-se que mudanças/alterações em Termos de Uso e Políticas de Privacidade sejam sempre comunicadas aos titulares de dados! (e-mail, banner pop-up etc.)

3) Contratos

A LGPD afirma que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados pessoais é de responsabilidade solidária entre o controlador e operador de dados pessoais. Ou seja, em qualquer contrato que haja o compartilhamento de dados pessoais, ambas as partes podem responder solidariamente por qualquer violação da LGPD.

Tendo em vista que os instrumentos contratuais vigentes não foram elaborados à luz da LGPD, as organizações precisarão definir uma estratégia para revisar/aditar tais documentos, de acordo com a relevância desses e deverão, em paralelo, passar a adotar instrumentos ou dispositivos contratuais que estejam de acordo com a legislação na celebração de novos negócios.

4) Manuais de processos internos existentes indicando atribuições e responsabilidades em relação ao tratamento de dados pessoais

Seção a ser inserida no Manual do Colaborador/Servidor da Organização, que tem por objetivo fornecer informações claras e precisas aos colaboradores/servidores da Organização acerca do tratamento de dados pessoais realizado pela Organização no contexto da relação empregatícia e gestão da rotina dos empregados/servidores.

6) Data Processing Agreement (DPA)

Um DPA é um contrato juridicamente vinculativo que estabelece os direitos e obrigações de cada parte em relação à proteção de dados pessoais. Estando sujeito à LGPD, é de seu interesse ter um DPA em vigor: primeiramente porque é necessário para a conformidade com a lei, mas o DPA também oferece garantias de que a outra parte (seja ela controladora ou operadora) é qualificada e capaz.

A LGPD determina que as partes envolvidas em uma atividade comum de tratamento de dados são solidariamente responsáveis pelos danos que tal atividade possa vir a causar aos titulares dos dados envolvidos. Como se trata de uma regra intransponível, a forma de a Organização se resguardar em face da outra parte na relação, caso danos aos indivíduos sejam causados, é justamente por meio de dispositivos contratuais que tenham o condão de :

- Garantir o direito de regresso da Organização em caso de responsabilização por ato ao qual não deu causa;
- Limitar a responsabilidade da organização em casos de violação, conforme aplicável

O que um DPA deve conter:

- O Operador deve concordar em tratar dados pessoais apenas com instruções escritas do Controlador.
- Todos que entram em contato com os dados estão comprometidos com a confidencialidade.
- Todas as medidas técnicas e organizacionais apropriadas são usadas para proteger a segurança dos dados.
- O Operador não subcontratará a outro Operador, a menos que seja instruído a fazê-lo por escrito pelo Controlador, caso em que outro DPA precisará ser assinado com o sub-operador.

7) Política de Retenção de Dados

É uma ferramenta no gerenciamento de todo ciclo de vida dos Dados Pessoais digitais e físicos. A política de retenção de dados determina através do cronograma por quanto tempo devemos manter os documentos de acordo com a base legal determinada pela LGPD (Lei Geral de Proteção de Dados – 13.709/18), aplicáveis à sua organização.

Esta Política deve se aplicar a todos profissionais ou prestadores de serviços da Organização que possam tratar dados pessoais.

É responsabilidade de todos familiarizarem-se com a Política e garantir o cumprimento adequado. Esta política se aplica a todas as informações usadas na Organização e serve como um controle administrativo para mitigar riscos à proteção e privacidade de dados.

Como a LGPD não determina um período de retenção, é recomendável que o período de retenção de cada documento seja analisado de acordo com a base legal e com os prazos prescricionais estabelecidos em lei.

8) Plano de Resposta à Incidentes

O Plano de Resposta à Incidentes serve para orientar o gerenciamento de qualquer incidente ou suspeita de incidente com dados que afetem a Organização ou qualquer de suas subsidiárias para garantir um gerenciamento célere e apropriado.

Um incidente de segurança pode ser definido como uma atividade ou conduta que afete a confidencialidade, a integridade ou disponibilidade dos dados.

Haverá um incidente de segurança quando um dado, não protegido, for: (i) acessado sem autorização; (ii) perdido; (ii) destruído; (iii) corrompido; (iv) divulgado indevidamente; ou se tornar indisponível (caso seja criptografado por um ransomware, por exemplo).

O Plano de Resposta a Incidentes deverá:

- Determinar o escopo e a gravidade do incidente
- Tomar medidas imediatas para conter o incidente

- Estabelecer um grupo de gestão de crise
- Documentação/Preservação de Evidências
- Identificar obrigações legais e contratuais
- Definir estratégia de comunicação
- Determinar periodicidade de reavaliação de cenários e riscos

9) Relatório de Impacto à Proteção de Dados (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:

- para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
- quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
- a qualquer momento sob determinação da ANPD (art. 38).

O RIPD deve conter, no mínimo:

- a descrição dos tipos de dados coletados
- descrição dos processos de tratamento de dados pessoais (que podem gerar riscos às liberdades civis e aos direitos fundamentais)
- a metodologia utilizada para a coleta e para a garantia da segurança das informações
- a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

10) Política de Cookies

Os cookies são arquivos de textos que têm o objetivo de identificar, coletar e armazenar diversos tipos de informações e dados sobre uma pessoa e o comportamento dela na internet. Estes cookies são considerados dados pessoais, uma vez que tornam as pessoas identificáveis, através das informações coletadas durante a navegação no site, sobre os dados e comportamento do usuário. Para estarmos em conformidade com a LGPD é necessário elaborarmos uma política de cookies.

Para construir uma boa política de cookies deve-se:

1. Reunir informações sobre os Cookies
   1.1. saber quais cookies seu site utiliza e como eles funcionam
   1.2. apontar a existência de cookies necessários, de desempenho, de funcionalidade e de publicidade
2. Explicar como as informações dos Cookies são usadas
   2.1. mostrar que a intenção ao colher os dados não é maliciosa, estando voltada apenas para entender e, a partir desse entendimento, otimizar a experiência no seu site.

3. Permitir que o usuário possa gerenciar os Cookies
   3.1. indicar a forma com que os cookies podem ser geridos permite que o usuário tenha maior controle sobre suas informações.

Para implementar a política de cookies deve-se:

- avisar aos visitantes/usuários da sua aplicação que existe uma política de cookies vigente (ou que ela foi atualizada).
- possibilitar excluir, revogar e permitir o uso dos cookies a qualquer tempo, com a ressalva dos cookies que são essenciais para o funcionamento da aplicação.
- gerar avisos e mensagens nas páginas que puderem ser acessadas informando a utilização de cookies e solicitando o consentimento do usuário.
- informar os impactos do não consentimento.

ORIENTAÇÕES IMPORTANTES DA ANPD PARA ÓRGÃOS PÚBLICOS

O anexo I do guia orientativo "TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO", versão 1.0 de janeiro/2022 nos traz uma tabela com recomendações quanto ao uso compartilhado de dados pessoais pelo Poder Público, conforme segue:

Requisito	Recomendação
Formalização e registro	• Instauração de processo administrativo; • Análise técnica e jurídica; • Decisão administrativa ou celebração de contrato, convênio ou instrumento congênere; • Edição de ato normativo interno.
Objeto e finalidade	• Descrição dos dados pessoais de forma objetiva e detalhada; • Indicação de finalidade específica; • Avaliação da compatibilidade entre a finalidade original e a finalidade do compartilhamento.
Base legal	• Indicação da base legal utilizada.
Duração do tratamento	• Definição do período (duração) do uso compartilhado dos dados, de forma fundamentada, e esclarecimento sobre a possibilidade de conservação ou a necessidade de eliminação após o término do tratamento.
Transparência e direitos dos titulares	• Divulgação das informações pertinentes na página eletrônica dos órgãos e das entidades responsáveis; • Divulgação de maneira que as informações sobre dados pessoais tratados pela entidade sejam de fácil compreensão; • Definição de responsabilidades e de procedimentos relativos ao atendimento de solicitações de titulares.
Prevenção e segurança	• Descrição das medidas técnicas e administrativas adotadas para proteger os dados pessoais de incidentes de segurança.
Outros requisitos (avaliação conforme o caso concreto)	• Autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais; • Ônus financeiro; • Requisitos específicos para compartilhamento de dados pessoais com entidades privadas (art. 26, § 1º e art. 27, LGPD); • Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; • Identificar as funções e responsabilidades dos agentes de tratamento.

Ainda, no mesmo guia orientativo, no anexo II são apresentados cuidados a serem observados quando há divulgação de dados pessoais pelo Poder Público, quais sejam:

Requisito	Recomendação
A coleta do dado pessoal é necessária e adequada para a finalidade do tratamento?	• Verificar a possibilidade de dispensa da coleta ou de eliminação dos dados pessoais, tendo em vista a sua efetiva necessidade para o alcance das finalidades do tratamento; • Verificar se há formas de atingir a finalidade almejada sem o tratamento de dados pessoais e de maneira menos gravosa para o titular de dados.
A divulgação envolve dados pessoais sensíveis?	• Em caso afirmativo, o tratamento deve ser efetuado com maior cautela, observando-se normas específicas, como os dispositivos da LGPD relativos a estudos em saúde pública.
Quais medidas de mitigação de risco para o titular de dados podem ser adotadas?	• Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; • Medidas de prevenção e segurança, a exemplo de anonimização ou pseudonimização dos dados pessoais sempre que isso não comprometa o exercício do controle social ; • Limitação da divulgação àqueles dados necessários para alcançar a finalidade pretendida , observados o contexto, a finalidade e as expectativas legítimas dos titulares; • Transparência do tratamento; e • Garantia de direitos dos titulares.

INICIATIVA PELA ELABORAÇÃO DA CARTILHA

FEDERAÇÃO DAS ASSOCIAÇÕES DE MUNICÍPIOS DO RIO GRANDE DO SUL – FAMURS

PRESIDENTE: Paulinho Salerno

SECRETARIA MUNICIPAL DE TRANSPARÊNCIA E CONTROLADORIA DE PORTO ALEGRE – SMTC

SECRETÁRIO: GUSTAVO FERENCI

CONSULTORIA TÉCNICA

ALLAN KOVALSCKI

SOBRE O AUTOR

Allan Machado Kovalscki, fundador da GCRC Desenvolvimento, graduado em Processos Gerenciais e Administração, MBA em Gestão Empresarial, Pós-MBA em Governança Corporativa e Risco, Pós Graduando em Ciência de Dados e Big Data Analytics, Pós Graduado em Gestão de Projetos, Pós Graduando LLM em Proteção de Dados: LGPD & GDPR. Atualmente ocupa também a função de Diretor Geral da COMPLY LGPD Solutions, Diretor Técnico – CTO na Armin GRC, é membro da RGB (Rede Brasil de Governança) nos comitês de LGPD e das estatais, foi membro do Comitê de Auditoria Estatutário do Grupo CEEE, sendo ainda professor e consultor na Fundação Universidade Empresa de Tecnologia e Ciências - Fundatec. Na Companhia Riograndense de Saneamento, empresa pública de economia mista, onde trabalhou por 20 anos, foi Superintendente de Controles Internos, Gestão de Riscos e Compliance, onde criou a área e implementou a metodologia e os processos de governança corporativa, gestão de riscos e compliance, foi Chefe do Departamento de Projetos e Processos, onde implementou o PMO da área de tecnologia na companhia e foi Superintendente de Tecnologia da Informação e Comunicação, tendo sido responsável pela implantação da Governança em TI, através do COBIT. Ainda, na Corsan, fez parte do Conselho Universitário e da Comissão de Ética. Possui certificação como DPO e certificações como Auditor Líder de Sistemas Integrados de Gestão em Compliance e Antisuborno, - Lead Assessor SIG ISO 19600:2014 e ISO 37001:2016, Gestão de Riscos e Continuidade de Negócios - Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019, Gestão da Segurança da Informação e Gestão de Privacidade da Informação - Lead Assessor SIG ISO 27001:2005 e ISO 27701:2019.

www.complylgpd.com.br
+55 51 3027-3344
comercial@lgpdcomply.com.br
+55 51 9943-0443