MELHORES RODOVIAS DO BRASIL
ABCR

GUIA DE BOAS PRÁTICAS PARA O ATENDIMENTO À LGPD NO SETOR DE CONCESSÃO DE RODOVIAS

MELHORES RODOVIAS DO BRASIL

ABCR

SUMÁRIO

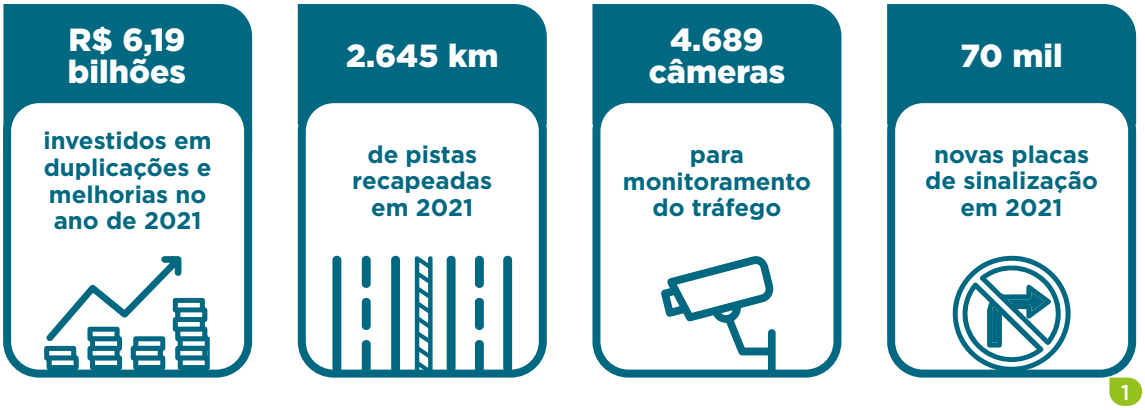
1. INTRODUÇÃO

Pensar a atividade pública, e assim a prestação do serviço público por todas as suas formas, inclusive por meio da exploração do bem público, requer conhecer tanto os meios de atuação do Estado quanto os modelos de interação existentes para atuação dos entes privados como prestadores do serviço público em substituição à administração.

Dadas as especificidades da prestação do serviço público por entes privados, como ocorre no caso das concessões rodoviárias, torna-se necessário compreender as regras e diretrizes legais e administrativas que abrangem as obrigações de todos os envolvidos, melhor condicionando o atendimento ao administrado, usuário do serviço público e destinatário final deste. Neste contexto a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18 - LGPD), ao estabelecer as diretrizes para o correto tratamento dos dados pessoais e dados pessoais sensíveis dos indivíduos (Titular dos dados pessoais), cuidou de destacar a atividade pública, assim compreendida a exercida direta ou indiretamente pelo Estado.

Considere-se a relevância das concessões rodoviárias pela sua magnitude, retratada na conjuntura que envolve a dimensão da malha rodoviária nacional, a quantidade de pessoas diretamente atendidas pelos serviços rodoviários, e o fato de ser esta a principal via de transporte utilizada no Brasil, tanto para deslocamento de pessoas quanto para o escoamento contínuo de grande parte da produção nacional.

Além da atratividade estrutural oferecida pelas concessionárias, com a contínua realização de melhorias (vide imagens abaixo), atualmente tornou-se indissociável deste conceito a necessidade de aplicação de processos de segurança dos ativos informacionais utilizados, gerados e geridos pelas empresas atuantes, como é o caso das informações e dados pessoais tratados durante a execução dos serviços públicos.



[1]

[1] Fonte: Melhores Rodovias do Brasil - ABCR - dados referentes a 2021

Voltar para o sumário

Assim, atendendo aos anseios dos usuários em reconhecer como são tratados seus dados pessoais durante a exploração da malha rodoviária pelas empresas concessionárias, bem como do interesse em compreender quais as melhores práticas a serem implementadas no que tange à privacidade e proteção dos dados pessoais durante a execução de suas atividades, convencionou-se a elaboração do presente Guia de Boas Práticas para o atendimento à LGPD no setor de concessão de rodovias, que aplicado em conjunto com as normas vigentes, visa aprimorar a segurança e o perfil de tratamento de dados pessoais pelas concessionárias de rodovias em todo o Brasil.

2. CONCESSÃO DOS SERVIÇOS PÚBLICOS

2.1. DEFINIÇÃO

A concessão é um instituto jurídico que permite ao Estado atribuir o exercício de um dado serviço público a outro ente (neste caso, privado) que aceite prestá-lo "em nome próprio, por sua conta e risco, nas condições fixadas e alteráveis unilateralmente pelo Poder Público, mas sob garantia contratual de um equilíbrio econômico-financeiro, remunerando-se pela própria exploração do serviço, em geral e basicamente mediante tarifas cobradas diretamente dos usuários do serviço".

Durante a prestação do serviço público **as concessionárias agem em nome próprio, respondendo assim pelos seus atos perante a Administração Pública e igualmente perante os administrados**, usuários do serviço público. Além do dever direto, as concessionárias também ficam obrigadas a conferir aos serviços explorados o padrão estabelecido pelas regras de Direito Administrativo para a atuação própria do Estado quando presta os mesmos serviços. Desta forma, a natureza jurídico-contratual das concessões, em especial por decorrerem de um imperativo de ordem pública, forçam as empresas concessionárias ao cumprimento de regras da esfera pública e da esfera privada.

2.2. PRINCÍPIOS

Dentre os padrões estabelecidos para prestação dos serviços públicos, alguns princípios da Administração Pública devem balizar o nível de serviço devido pelo ente privado, sem prejuízo de outras disposições contratuais previamente estabelecidas.

Assim, as concessionárias devem obedecer ao princípio da **legalidade**, agindo sempre nos termos das normas aplicáveis à execução dos serviços concedidos, durante a sua realização. Igual sentido se faz da necessidade de cumprir o princípio da **impessoalidade**, através do qual determina-se que o oferecimento do serviço público deve ser igualitário a todos os cidadãos, sem oferecimento de privilégios a alguns em detrimento de outros, algo intimamente relacionado aos conceitos de privacidade e proteção de dados, objetos deste Guia.

Ainda cabe às concessionárias atender ao princípio da **moralidade**, prestando o serviço público concedido de forma ética e conforme os preceitos da moral, válidos ao momento da prestação. A **publicidade**, outro princípio da Administração Pública a ser observado pelo ente privado durante a concessão, estabelece o dever de transparência e prestação de contas relacionados à exploração do patrimônio público. Por fim, o princípio da **eficiência**, por meio do qual exige-se do Estado o uso coerente dos recursos públicos, atinge as concessionárias na própria fiscalização do ente público quanto a correta e justa execução dos serviços concedidos ao ente privado.

2.3. DISPOSIÇÃO LEGAL E DEMAIS RESPONSABILIDADES

A possibilidade de transferência da execução do serviço público pelo Estado ao ente privado, bem como todos os desdobramentos oriundos deste modelo, decorre do artigo 175 da Constituição Federal, o qual dispõe que "**incumbe ao Poder Público**, na forma da lei, **diretamente ou sob regime de concessão ou permissão**, sempre através de licitação, **a prestação de serviços públicos**."

O referido artigo 175 da Constituição Federal foi inicialmente regulamentado por força da Lei nº 8.987/95, que dispõe sobre o regime de concessão e permissão da prestação de serviços públicos, e que estabelece os principais parâmetros para estabelecimento deste modelo de relação público-privada. A mencionada Lei, em seu artigo 25, inclusive, cuida de reforçar que a concessionária é responsável pela execução do serviço concedido, **respondendo por todos os prejuízos causados ao poder concedente, aos usuários ou a terceiros**, sem que a fiscalização exercida pelo órgão competente exclua ou atenue essa mesma responsabilidade.

Além Lei nº 8.987/95, a Lei nº 11.079/04 tratou de estabelecer inovação aos padrões de licitação através da criação do modelo de contratação via parceria público-privada no âmbito da Administração Pública, diferenciando-se este formato pelo perfil de contrapartidas que estruturam sua aplicação.

Em ambos os casos, independentemente da esfera em que ocorra a concessão (Federal ou Estadual), com o advento da LGPD as concessionárias passaram a ter a necessidade de estarem adequadas aos ditames legais da proteção de dados pessoais, devendo interpretar a norma vigente de forma a garantir o correto e seguro tratamento dos dados pessoais necessários à execução dos serviços explorados.

3. ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

3.1. ESCOPO DE APLICAÇÃO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18), também conhecida por LGPD, é a legislação que regula o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural (pessoa física), ou seja, o titular de dados.

Em outras palavras, a LGPD estabelece as "regras do jogo" para tudo que é feito com informações de pessoas físicas.

A LGPD se aplica a qualquer tratamento de dados pessoais, realizado em meio físico ou digital, por pessoa física ou jurídica de direito público ou privado.

Exemplos:

Dados em meio físico: formulários de cadastramento, cópias impressas, currículos em papel, rascunho, arquivos físicos, etc.

Dados em meio digital: cópias digitais, documentos em e-mail, WhatsApp, dados inseridos em CRM/ERP, sistemas internos, biometria, informações em planilhas, etc.

!

ATENÇÃO:

Nos termos do art. 4º da LGPD, a legislação não se aplica quando o tratamento for: (i) realizado por pessoa física para fins particulares e não econômicos; (ii) realizado para fins exclusivamente jornalístico, artísticos ou acadêmicos; (iii) realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; e, (iv) provenientes de fora do território nacional e que não sejam objeto de comunicação e uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Nesse contexto, surge o questionamento: Quais são as obrigações da concessionária?

A concessionária que realizar o tratamento de dados pessoais deverá, em resumo:

- Cumprir os princípios da LGPD;
- Registrar e fundamentar cada operação de tratamento de dados conforme as bases legais;
- Manter os dados pessoais seguros e armazenados pelo tempo necessário;
- Atender aos direitos dos titulares;
- Adotar medidas técnicas e administrativas aptas a proteger os dados pessoais da ocorrência de violação de dados pessoais, garantindo sempre a segurança da informação nos tratamentos realizados; e
- Comunicar à ANPD e aos titulares envolvidos as violações de dados pessoais que acarrete risco ou dano relevante ao titular.

3.2. CONCEITOS

Apresentamos abaixo os conceitos básicos e necessários para entender os fundamentos e disposições trazidas pela Lei Geral de Proteção de Dados Pessoais (LGPD):

- **Agente de Tratamento:** O controlador e o operador.
- **ANPD:** Acrônimo para Autoridade Nacional de Proteção de Dados, órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável.

- **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, ao Titular dos Dados Pessoais.

- **Controlador:** Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, como os meios e finalidades de tratamento. Por exemplo, concessionárias de rodovias.

- **Dado Pessoal:** Qualquer informação que identifique ou permita identificar uma pessoa física, diretamente ou indiretamente. Como por exemplo, o nome, RG, CPF, endereço, e-mail, localização, identidade funcional, placa de veículo, cargo, filiação, dados comportamentais etc.

- **Dado Pessoal Sensível:** Também são informações que identificam ou permitam identificar uma pessoa, mas que, pela sua natureza, a lei exige maior cautela e proteção, como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- **Encarregado pelo tratamento de Dados Pessoais:** Pessoa física ou jurídica indicada pela concessionária e que atua como canal de comunicação entre a concessionária e os titulares dos dados pessoais e a ANPD. O encarregado deve orientar o controlador, bem como os colaboradores sobre as normas e políticas internas de proteção de dados e deve ser apoiado pela alta direção para o exercício de suas funções.

- **Medidas de segurança:** são as medidas destinadas a proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, quando o tratamento implicar transferência de dados, e contra qualquer outra forma de tratamento ilícito. São exemplos de medidas de segurança a utilização de criptografia, antivírus e anti-malware, a pseudonimização e demais medidas de segurança administrativas, técnicas e físicas apropriadas e suficientes para proteger a confidencialidade, integridade e disponibilidade dos dados pessoais mantidos, consultados ou transmitidos.

- **Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador, não podendo extrapolar aquilo que lhe é autorizado, sob pena de atrair obrigações e as-

sumir responsabilidades pelas violações contratuais. Por exemplo, empresas de serviço de armazenamento em nuvem.

- **Pseudonimização:** é o tratamento por meio do qual um dado 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.

- **Relatório de Impacto à Proteção de Dados (RIPD):** Documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- **Titular dos dados pessoais:** Pessoa física a quem se referem os dados pessoais que são objeto de tratamento, como por exemplo colaboradores, usuários, visitantes, prestadores de serviço, entre outros. São considerados como titulares vulneráveis pela LGPD e regulamentação da ANPD, as crianças, adolescentes e idosos.

- **Tratamento de Dados Pessoais:** Toda e qualquer operação realizada com dados pessoais, como as que se referem, mas não se limitam, à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Por exemplo, arquivar documentos em pastas físicas ou digitais.

- **Violação de Dados Pessoais:** Destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a Dados Pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

3.3. PRINCÍPIOS

O tratamento de dados pessoais deve sempre se dar de boa-fé e atender aos seguintes princípios previstos no art. 6º da LGPD:

- **Finalidade:** o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com as finalidades originalmente vinculadas ao tratamento;

- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto;

- **Necessidade (ou minimização):** tratamento apenas do mínimo de dados necessários e pelo tempo necessário para a alcance das finalidades, não podendo ser os dados excessivos;

- **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;

- **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;

- **Transparência:** informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento ao titular, observados os segredos comercial e industrial;

- **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;

- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e,

- **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais.

3.4. BASES LEGAIS DE TRATAMENTO

As bases legais são as hipóteses capazes de tornar o tratamento de dados pessoais válido, segundo a LGPD. Para o tratamento de dados pessoais, aplicam-se as hipóteses previstas no art. 7º da LGPD e, para o tratamento de dados pessoais sensíveis, aplicam-se as hipóteses previstas no art. 11 da LGPD.

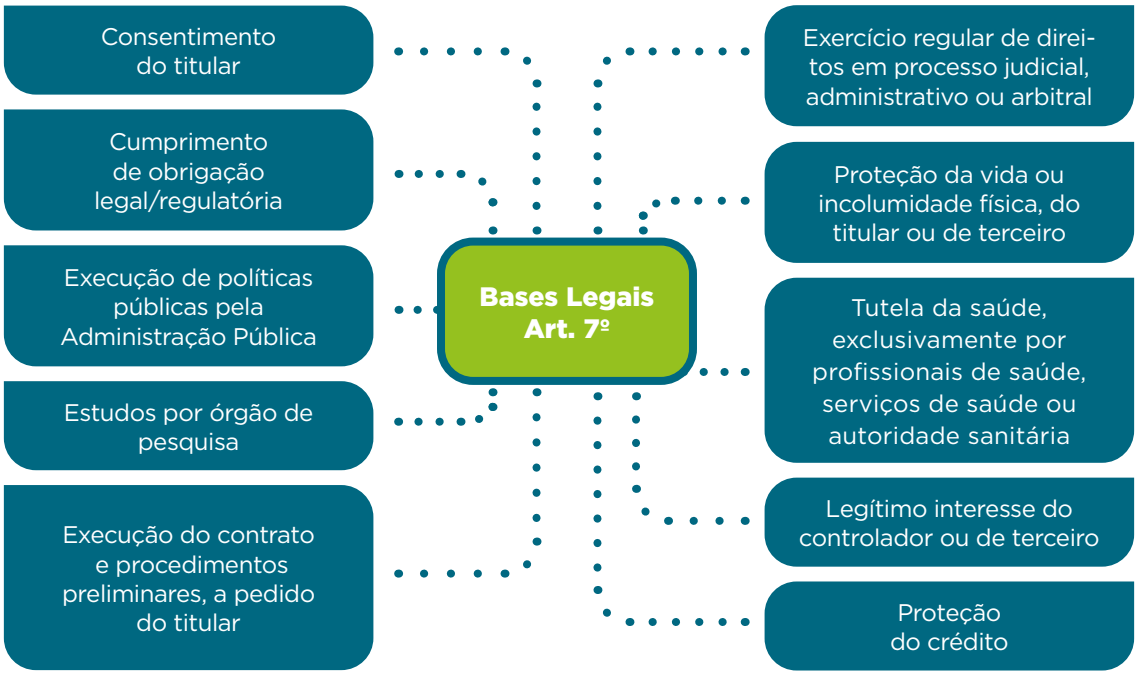
Dessa forma, as concessionárias devem realizar o tratamento de dados pessoais amparada em uma das bases legais estabelecidas pela LGPD.

!

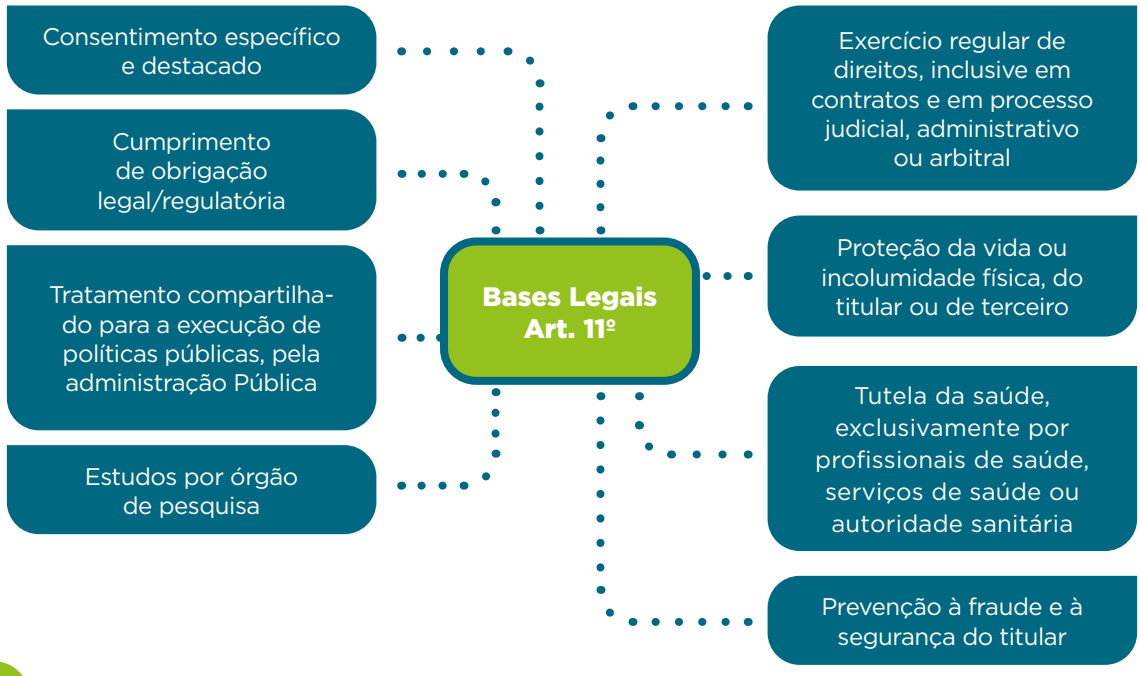
ATENÇÃO:

As bases legais não possuem hierarquia entre si. A escolha da base mais adequada ocorre conforme a finalidade pretendida com o tratamento. Assim, não há prevalência, por exemplo, do consentimento sobre outras bases legais.

São as bases legais para o tratamento de dados pessoais (Art. 7º da LGPD):



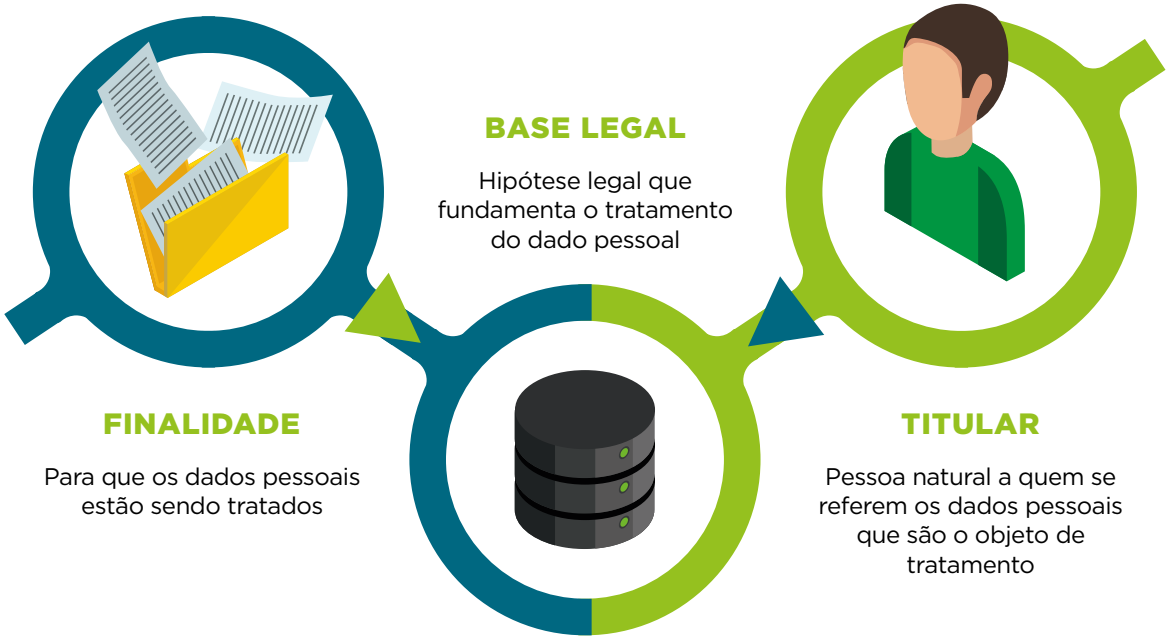
São as bases legais para tratamento de dados pessoais sensíveis (Art.11 da LGPD):



ATENÇÃO:

O tratamento de dados sensíveis não pode se dar com base no **legítimo interesse** e nem para **proteção ao crédito**.

Para que a base legal seja aplicada ao tratamento de dados pessoais de forma correta, faz-se necessário identificar qual é a finalidade específica do tratamento, a categoria dos titulares e a natureza dos dados pessoais tratados.



Cada finalidade constituirá um fluxo de dado pessoal e, por conseguinte, deverá ter uma base legal aplicada. A mesma regra aplica-se à categoria de titular, que a depender da relação jurídica estabelecida com a Concessionária, pode alterar a base legal ainda que a finalidade do tratamento seja a mesma.

Bases legais no contexto das atividades realizadas pelas Concessionárias:

Consentimento (Art. 7º, I e Art. 11, I da LGPD):

Segundo o artigo 5º, inciso XII da LGPD, o consentimento é considerado como a manifestação livre, informada e inequívoca para uma finalidade específica. Pode ser fornecido por escrito (em cláusula destacada) ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8º, LGPD).

Importa destacar que o consentimento pode ser revogado a qualquer tempo pelo titular, situação em que o controlador deverá cessar a atividade de tratamento caso não possua outra base legal aplicável ao tratamento. Ainda, cabe ao controlador o ônus da prova de que o consentimento foi coletado nos termos e forma da Lei.

Exemplo: Registro no newsletter da concessionária.

Cumprimento de Obrigação Legal/Regulatória (Art. 7º, II e Art. 11, II, "a" da LGPD):

Sempre que a finalidade do tratamento dos dados pessoais seja realizada para o cumprimento de uma obrigação legal ou regulatória, a base aplicada será a do art. 7º, II e art. 11, II, a da LGPD.

Exemplo: Monitoramento de rodovias federais: Resoluções nº 2.064/2007 e nº 3.576/2010 da ANTT.

Execução de Políticas Públicas pela Administração Pública (Art. 7º, III e Art. 11, II, "b" da LGPD):

Trata-se de base legal utilizável pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Execução de Contrato e Atividades Preliminares (Art. 7º, V e Art. 11, II, "d" da LGPD):

Tais bases serão utilizadas quando a finalidade do tratamento dos dados pessoais seja para a execução do contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Importa destacar que o contrato que baseia o tratamento deve necessariamente conter o titular como parte. Ainda, faz-se necessário identificar se a finalidade estabelecida realmente é necessária a execução do contrato em questão. Caso contrário, o tratamento deverá ser legitimado em outra base legal.

Exemplo: Pagamento de colaboradores e prestadores de serviço (Contrato de Trabalho e Contrato de Prestação de serviço); Liberação de acesso a colaboradores e prestadores de serviço (Contrato de Trabalho e Contrato de Prestação de serviço).

Exercício regular de direitos em processo judicial, administrativo ou arbitral (Art. 7º, VI e Art. 11, II, "d" da LGPD:

Trata-se de base legal utilizada pelas concessionárias para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Exemplo: Defesa em processo judicial.

Proteção da Vida ou Incolumidade Física de Terceiro (Art. 7º, VII e Art. 11, II, "e" da LGPD):

Trata-se de base legal que pode ser utilizada pela concessionária quando o tratamento de dados pessoais for realizado com a finalidade de proteção da vida da incolumidade física do titular ou de terceiro.

Exemplo: Encaminhamento de visitante da concessionária a um hospital em caso de emergência.

Tutela da Saúde (Art. 7º, VIII e Art. 11, II, "f" da LGPD):

Trata-se de base legal destinada a legitimar o tratamento de dados pessoais para a tutela da saúde do titular. Entretanto, tal tratamento deve ser realizado exclusivamente por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Exemplo: Atendimento prestado pelo médico do trabalho da concessionária ao colaborador.

Legítimo Interesse (Art. 7º, IX da LGPD):

Nos termos do art. 10 da LGPD, o legítimo interesse do controlador somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam ao apoio e promoção de atividades do controlador e à proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas suas legítimas expectativas e os direitos e liberdades fundamentais, nos termos desta Lei.

Referida base legal só poderá ser utilizada quando o legítimo interesse da Concessionária não se sobressair aos direitos e liberdades fundamentais do titular dos dados pessoais. Trata-se de uma base que poderá legitimar apenas o tratamento de dados pessoais, excluindo o tratamento os dados pessoais sensíveis.

Exemplo: Controles de acesso de visitantes; Liberação de Wi-fi para terceiros.

Prevenção à fraude e à Segurança do titular (Art. 11, II, "g" da LGPD):

A base de garantia da prevenção à fraude, pressupõe a execução processos de identificação e autenticação de cadastro em sistemas eletrônicos, como o reconhecimento facial, biometria, entre outros. Trata-se de uma base que poderá legitimar apenas o tratamento de dados pessoais sensíveis.

Exemplo: Liberação de entrada às dependências da concessionária por biometria facial.

REGISTRO DAS ATIVIDADES DE TRATAMENTO (ROPA)

Para que a concessionária possua um controle de todas as atividades de tratamento de dados pessoais realizadas, é importante que tenha o Registro das Atividades de Tratamento, também conhecido como ROPA (Records of Processing Activities).

O ROPA é uma das obrigações atribuídas ao controlador e operador pela LGPD. Sua necessidade decorre de disposições tanto do GDPR (Art. 30) quanto da LGPD (Art. 37):

> **Art. 37.** O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

O ROPA é um documento importante que suporta o programa de proteção de dados e permite à organização ter visibilidade em relação aos seus processos/fluxos que envolvem dados pessoais. Embora a LGPD não tenha indicado o que deve conter no ROPA, o GDPR trata da questão em seu art. 30, indicando que:

> **Artigo 30 – Registro das atividades de tratamento**
>
> **1.** Cada responsável pelo tratamento (controlador) e, sendo caso, o seu representante deverá manter registro de todas as atividades de tratamento sob a sua responsabilidade. Desse registro devem constam as seguintes informações:
>
> **a)** O nome e os contatos do responsável pelo tratamento e, sendo caso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
>
> **b)** As finalidades do tratamento dos dados;
>
> **c)** A descrição das categorias de titulares de dados e das categorias de dados pessoais;

> **d)** As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
>
> **e)** Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49, n 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;
>
> **f)** Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
>
> **g)** Se possível, uma descrição geral das medidas técnicas e organizacionais no domínio da segurança referidas no artigo 32, n 1.

Assim, considerando que a Autoridade Nacional de Proteção de Dados (ANPD) ainda não regulamentou o tema, recomenda-se que o ROPA contenha as informações acima indicadas como demonstração de melhores práticas em governança de dados pessoais.

Por fim, considerando que as atividades realizadas pelas concessionárias são dinâmicas e podem mudar constantemente, o ROPA deve ser um documento "vivo" dentro da organização de forma a retratar de forma atualizada as atividades de tratamento de dados pessoais.

Dessa forma, recomenda-se que referido documento seja revisitado sempre que um sistema for alterado, quando um novo fluxo for incorporado aos procedimentos ou quando as atividades já mapeadas forem alteradas ou atualizadas.

BASE LEGADA

Base legada é o conjunto de dados pessoais constituído anteriormente à entrada em vigor da LGPD. Nos termos do art. 63 da legislação, a ANPD deverá estabelecer normas sobre a adequação destas bases, tema que ainda está pendente de regulamentação.

De toda forma, a manutenção de base legada configura operação de tratamento de dados pessoais, ainda que seja de mero armazenamento, devendo, por isso, ser adequada.

Para que isso seja feito, é necessário que as bases legadas sejam alvo de levantamento, avaliação e análise para verificação do cumprimento dos requisitos da lei, especialmente quanto à atribuição das hipóteses de tratamento cabíveis. Neste sentido, apresentamos as seguintes recomendações para não correr riscos de não conformidade, bem como de evidenciar a boa-fé da Concessionária em adequar todos seus processos de tratamento de dados pessoais com a Legislação:

PASSO A PASSO

Passo 1
Levantar a qualidade e quantidade dos dados pessoais dos titulares na base legada;

Passo 2
Levantar se os dados pessoais tratados são necessários para as finalidades mapeadas;

Passo 3
Realizar o (re-)enquadramento das hipóteses de tratamento dos fluxos de dados pessoais;

Passo 4
Levantar prova de consentimento (se necessário) no que diz respeito ao tratamento dos dados pessoais;

Passo 5
Verificar possibilidade de anonimizar os dados pessoais e dados pessoais sensíveis tratados;

Passo 6
Suspender o tratamento dos dados pessoais de titulares (pode ser mantido em um repositório do tipo quarentena até que haja algum pronunciamento da ANPD a respeito do tema).

3.5. TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Os dados pessoais de crianças e adolescentes possuem indicações específicas na LGPD, em seção própria da legislação (Capítulo II, Seção III – Do Tratamento de Dados Pessoais de Crianças e Adolescentes), de forma a garantir a legitimidade do tratamento de dados pessoais.

No entanto, para melhor compreensão das disposições ali previstas, é essencial delimitar-se o que a legislação brasileira considera criança e adolescente. Para isso, utiliza-se como referência nacional a previsão do artigo 2º da Lei nº 8.069, de 1990, também conhecida como Estatuto da Criança e do Adolescente (ECA):

> Considera-se criança, para os efeitos desta Lei, a **pessoa até doze anos de idade incompletos**, e **adolescente aquela entre doze e dezoito anos de idade**.

A LGPD prevê, em seu artigo 14, que o tratamento de dados pessoais de crianças e adolescentes "deverá ser realizado em seu melhor interesse" e, no caso de tratamento de dados pessoais de crianças (menores até doze anos incompletos), o parágrafo primeiro do referido artigo dá a entender pela necessidade do consentimento específico e em destaque fornecido por pelo menos um dos pais ou pelo responsável legal. Ainda, há a previsão de dispensa de consentimento quando a coleta dos dados for necessária para contatar os pais ou o responsável legal, uma única vez e sem armazenamento, ou para sua proteção, nos termos do parágrafo terceiro.

Entende-se que o tratamento de dados pessoais tanto de crianças, como de adolescentes, pode ser legitimado em quaisquer bases legais constantes nos artigos 7º e 11 da LGPD em combinação com o artigo 14 da LGPD, situação em que se deve realizar uma análise detalhada quanto ao melhor interesse.

Assim, quando a base legal for o consentimento, este deve ser coletado na forma do parágrafo primeiro do artigo 14 da LGPD, ou seja, "específico e em destaque dado por pelo menos um dos pais ou responsável legal".

Vale ressaltar, que a XI Jornada de Direito Civil, em seu Enunciado nº 684 reforçou referido entendimento, ao dispor que o art. 14 da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) não exclui a aplicação das demais bases legais, se cabíveis, observado o melhor interesse da criança.

Diante disso, é possível a utilização de outras bases legais que não o consentimento para o tratamento de dados pessoais de crianças.

3.6. DIREITO DOS TITULARES

A LGPD é uma legislação principiológica que possui como objetivo principal a proteção de direitos e garantias fundamentais como a liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, ou seja, do titular.

Ainda, traz como um de seus fundamentos a autodeterminação informativa, que se caracteriza no poder do titular de decisão a respeito do tratamento de seus dados pessoais. Nesse sentido, verifica-se que a LGPD trouxe uma série de proteções e poderes aos titulares de dados pessoais, em especial seus direitos, que estão previstos no Capítulo III.

!

ATENÇÃO:

Importante notar que para além dos Titulares de dados pessoais tidos como comuns à atividade das concessionárias, neste caso os usuários finais dos serviços prestados, estas também realizam o tratamento de dados pessoais orgânico na relação que possuem com seus colaboradores. Por tal questão, os programas de privacidade e proteção de dados das empresas envolvidas devem contemplar a adoção de medidas que visem estabelecer diretrizes para o correto tratamento dos dados pessoais envolvidos nas relações empregatícias de costume, em especial, mas sem prejuízo de outros necessários, estabelecendo procedimentos que que contenham os controles aplicados aos trabalhos executados em home office (como são exemplos as imposições de regras para realização de acesso remoto; uso de recursos de tecnologia da informação e comunicação; aplicação de termo de responsabilidade para uso de equipamentos fora das dependências das concessionárias; gestão de tempo; gestão remota de acessos, entre outros), bem como para os serviços realizados in loco, como na transparência quanto ao monitoramento interno e suas limitações. Outrossim, as concessionárias devem atentar-se à necessidade de orientar e gerar transparência para seus colaboradores, seja por meio de campanhas de conscientização e aviso de privacidade ou atualização de seus contratos de trabalho para que nestes constem as designações relacionadas à proteção de dados pessoais no sentido de esclarecer como os empregadores realizam, na qualidade de Controladores, o tratamento de dados pessoais dos colaboradores (aqui, Titulares).

Conforme a LGPD, o titular poderá solicitar do controlador, a qualquer momento e mediante requisição:

- A **confirmação da existência de tratamento**: o titular tem o direito de saber se a empresa trata seus dados;
- O **acesso aos dados**: o titular poderá obter cópia de seus dados pessoais;
- A **correção** de dados incompletos, inexatos ou desatualizados;
- A **anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- A **portabilidade** dos dados a outro fornecedor (pendente de regulação pela ANPD);
- A **eliminação** dos dados tratados com base no consentimento;
- **Informação** das entidades públicas e privadas com as quais a empresa compartilhou dados;
- **Informação** sobre a possibilidade de não fornecer consentimento e consequências da negativa;
- A **revogação do consentimento**: tão simples quanto o consentimento pode ser concedido, poderá ele ser retirado a qualquer momento;
- **Petição contra o controlador** perante a Autoridade Nacional de Proteção de Dados (ANPD);
- **Oposição** a tratamento que descumpra a lei;
- **Revisão** de decisão tomada unicamente com base em tratamento automatizado de dados pessoais.

!

ATENÇÃO:
Nota-se que a LGPD trouxe a obrigação de atendimento à requisição de direito dos titulares ao controlador. Contudo, considerando que existem relações contratuais nas quais o operador que possui o contato direto com titular (como por exemplo a terceirização do "fale conosco"), faz-se necessário uma adequação contratual no sentido de estabelecer o dever de cooperação para recebimento, processamento e resposta à requisição de direito, estabelecendo prazos e deveres, haja vista a possibilidade de imposição de sanções quando do descumprimento ao Capítulo III da LGPD, assim como a possibilidade de judicialização do caso pelo titular.

Como atender aos direitos dos titulares?

A LGPD não estabeleceu um formato para o atendimento dos direitos dos titulares, entretanto, em linha com as orientações da ANPD em guias publicados, recomenda-se a criação de um canal de comunicação específico para o atendimento ao titular, de forma a facilitar o recebimento, processamento e resposta destas requisições. Geralmente, observa-se a indicação de um e-mail ou portal próprio no Aviso/Política de Privacidade constante no site da concessionária.

Nesse sentido, é importante que a concessionária estabeleça um canal que seja efetivo, em termos de atendimento, organização, acompanhamento e respostas. Ainda, a uma equipe responsável deve ser capaz de realizar a gestão das requisições, como forma de controlar os prazos de respostas e a evitar que as solicitações fiquem dispersas em setores na organização.

Como forma de otimizar o processo, existem no mercado hoje, ferramentas que podem ser implementadas para o acompanhamento e atendimento automatizado das requisições de direito dos titulares.

Qual é o prazo para atendimento à solicitação do titular?

A LGPD estabeleceu um prazo de até 15 (quinze) dias, a contar da data de recebimento, para atendimento à confirmação de existência e ao acesso a dados pessoais. Quanto aos demais, ainda que a ANPD não tenha se pronunciado a respeito, é recomendável que seja adotado o mesmo prazo de 15 dias para a devida tratativa.

Ressalta-se que a ANPD poderá dispor de forma diferenciada acerca dos prazos, para os setores específicos.

O que deve constar na resposta ao direito de acesso?

Ainda que os artigos 18 e 19 da LGPD, que tratam do direito de acesso não tenham indicado o que deve ser fornecido ao titular, o art. 9º da legislação estabelece que o titular possui o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da:

- Finalidade específica, forma e duração do tratamento, observados os segredos comercial e industrial;
- Identificação e informações de contato do controlador;
- Informações acerca do uso compartilhado de dados pelo controlador e a

finalidade do compartilhamento;

- Quais as responsabilidades dos agentes que realizam o tratamento dos dados pessoais; e
- Quais são os direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Para auxílio ao atendimento do direito de acesso, o Registro das Atividades de Tratamento (ROPA – Records of Processing Activities) é de extrema importância para a organização. Isso porque, como já abordado no presente Guia, no ROPA constam informações importantes acerca dos fluxos de tratamentos de dados realizados.

!

ATENÇÃO:

O atendimento de solicitação do Titular deve ser precedido da confirmação da identidade do solicitante, no sentido de verificar se a pessoa que está realizando o pedido é realmente quem diz ser, como forma de evitar a ocorrência de um incidente de dados pessoais, como o compartilhamento indevido de dados.

Como estruturar o atendimento às requisições de direitos dos titulares?

PASSO A PASSO

Passo 1
Manter o Registro das Atividades de Tratamento (ROPA) atualizado;

Passo 2
Designar um responsável pelo recebimento e atendimento das requisições ou terceirizar a gestão das requisições;

Passo 3
Confirmar a identidade do titular;

Passo 4
Análise pelo Encarregado pelo Tratamento de Dados Pessoais para verificar se a requisição atende os requisitos formais.

3.7. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

A Transferência Internacional de dados pessoais caracteriza-se na transferência de dados para um país estrangeiro ou organismo internacional do qual o país seja membro. A transferência internacional pode ocorrer mediante uma ação ativa – por exemplo, quando a concessionária encaminhar dados pessoais para outras empresas que se localizam fora do país – bem como, por uma ação passiva, por exemplo o armazenamento de dados pessoais em serviços de nuvem, que possuem servidores estabelecidos em outros países.

Com o objetivo de certificar ao titular de dados que tem suas informações transferidas para o exterior a mesma proteção e zelo garantidos na legislação brasileira, a LGPD, em seu Capítulo V, estabelece alguns mecanismos para que a transferência seja permitida:

> Art. 33. A **transferência internacional de dados pessoais somente é permitida** nos seguintes casos:
>
> I - para **países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado** ao previsto nesta Lei;
>
> II - quando o **controlador oferecer e comprovar garantias de cumprimento** dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a **transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução**, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária **para a proteção da vida ou da incolumidade física do titular ou de terceiro**;
>
> V - quando a **autoridade nacional autorizar a transferência**;
>
> VI - quando a transferência resultar em **compromisso assu-**

> **mido em acordo de cooperação internacional**;
>
> VII - quando a transferência for necessária para a **execução de política pública ou atribuição legal do serviço público**, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu **consentimento específico e em destaque para a transferência**, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Todavia, é importante observar que parte das hipóteses tuteladas no dispositivo ainda não podem ser exercidas, uma vez que carecem de regulamentação pela ANPD, como é o caso da definição de conteúdo de cláusulas-padrão (artigo 35), que está sob sua responsabilidade, bem como a avaliação do nível de proteção de dados do país terceiro, que também ficará a cargo da Autoridade.

Vale mencionar que no Relatório Semestral de Acompanhamento da Agenda Regulatória publicado pela ANPD, o assunto já foi indicado como projeto prioritário e em andamento nas reuniões e estudos internos conduzidos pela sua equipe técnica[2].

Portanto, enquanto algumas das medidas previstas no artigo supracitado ainda não podem ser homologadas pela ANPD, é recomendável que as concessionárias se atenham às seguintes hipóteses permissivas para a realização de transferência internacional de dado pessoais:

- Utilização de cláusulas contratuais específicas para determinada transferência;
- Consentimento específico e em destaque do titular para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente de outras finalidades;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para cumprimento de obrigação legal ou regulatória; ou
- Para a execução de contrato ou exercício regular de direitos.

A adoção de cláusulas contratuais específicas que ofereçam e comprovem

[2] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/publicado-relatorio-semestral-de-acompanhamento-da-agenda-regulatoria

o correto cumprimento dos princípios e direitos dos titulares de dados previstos na LGPD atualmente é a opção mais recomendável para a adequação e legitimação da transferência internacional de dados pessoais.

!

ATENÇÃO:

Para uma melhor adequação desses contratos, recomenda-se que as cláusulas contratuais específicas sejam elaboradas com embasamento nas cláusulas contratuais padrão já autorizadas pela Comissão Europeia[3], a fim de garantir as boas práticas já adotadas internacionalmente e que, muito provavelmente, serão adotadas no Brasil.

Por fim, em atendimento ao princípio da transparência, é de suma importância que os titulares de dados tenham ciência acerca da realização de transferência internacional por parte das concessionárias.

E como conceder a transparência ao titular nesses casos?

- Por meio dos contratos firmados;
- Através de adequação de políticas internas (no caso de colaboradores); e,
- Por meio de Políticas/Aviso de Privacidade.

[3] Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en

3.8. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Para garantia da conformidade das Concessionárias, faz-se de extrema importância a nomeação de um Encarregado pelo Tratamento de Dados Pessoais, também conhecido como DPO (Data Protection Officer), em consonância ao art. 41 da LGPD.

Nos termos do inciso VIII do art. 5º da LGPD, o encarregado 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).

Considerando as boas práticas internacionais, conforme o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[4]:

> "O encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica. Recomenda-se que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviços ou um ato administrativo."

Quanto às **qualificações profissionais** do Encarregado, é recomendável que o profissional conheça o setor de atuação da Concessionária, bem como tenha domínio da legislação de proteção de dados e tenha conhecimento sobre tecnologia, padrões de segurança (ISOs) e de governança de dados (DAMA).

As pessoas que atuam nesta área costumam ter uma carreira e experiência prévia nas áreas jurídica, de tecnologia da informação, auditoria e/ou compliance, não havendo, no entanto, obrigatoriedade de formação nessas áreas de conhecimento.

O Encarregado também deverá ter **habilidades** em soft skills e saber transitar pelas diversas áreas da concessionária e, acima de tudo, ter o suporte da Alta Direção, como forma de fortalecer sua atuação e aumentar a cooperação dos demais colaboradores, sendo envolvido em todas as operações que envolvam o tratamento de dados pessoais.

Para que o Encarregado cumpra com seus objetivos, há a necessidade de a concessionária fornecer recursos necessários ao desempenho de suas atividades e à atualização de seus conhecimentos. Dentre os recursos e suporte que a Concessionária deverá garantir e fornecer ao Encarregado, destacamos os seguintes:

- Apoio efetivo às atividades do Encarregado pelo mais alto nível de gestão,

[4] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

inclusive, quando aplicável, do Conselho de Administração;

- Não penalização do Encarregado em razão do cumprimento de suas atividades relacionadas à proteção de dados pessoais, sendo a responsabilidade do Encarregado limitada ao bom exercício de sua função consultiva;
- Garantir que outras atividades exercidas pelo Encarregado dentro da concessionária, caso ele exerça alguma outra função além de Encarregado, não gerem um conflito de interesses;
- Alocação de recursos humanos para formação da equipe de apoio, assim como recursos financeiros tanto para o orçamento interno dos custos rotineiros do Encarregado quanto para eventual contratação de consultores e advogados externos e de plataformas operacionais;
- Disponibilização de infraestrutura adequada, local de trabalho, salas privativas para condução de reuniões e entrevistas que possam abordar matérias sensíveis e sigilosas;
- Comunicação oficial sobre a nomeação do Encarregado, inclusive mediante disponibilização dos canais oficiais para contato, preferencialmente, mas não exclusivamente, na página da concessionária na internet;
- Capacitação e formação contínua, viabilizando que o Encarregado esteja sempre atualizado com relação à proteção de dados e matérias relacionadas; e
- Garantir que as recomendações, observações e considerações do Encarregado sejam levadas em conta nas decisões internas, registrando e fundamentando os casos em que tais recomendações não sejam acatadas.

ATIVIDADES E RESPONSABILIDADES DO ENCARREGADO

De acordo com o art. 41 da LGPD, o Encarregado possui as seguintes atividades:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além destas, percebe-se que o Encarregado é importante para todo o ecossistema de proteção de dados pessoais das Concessionárias, razão pela qual

destacam-se atribuições adicionais:

- Prestar consultoria, quando lhe for solicitado;
- Tomar as medidas necessárias para promover a cultura sobre proteção de dados pessoais dentro da organização, por meio de treinamentos periódicos, palestras, informativos internos, dentre outras atividades;
- Gerir a governança de dados pessoais, de forma a controlar a conformidade das atividades de tratamento com as leis e políticas internas de proteção de dados aplicáveis;
- Gerir incidentes de segurança da informação com dados pessoais;
- Auxiliar na contratação e fiscalização de terceiros, verificando o nível de aderência do terceiro em privacidade e segurança da informação.
- Emitir pareceres sobre a necessidade de elaboração e atualização dos Relatórios de Impacto à Proteção de Dados Pessoais (DPIA).

Importante frisar que a estrutura de governança em proteção de dados pessoais de uma organização pode ser variável, a depender da complexidade das operações, do porte da organização, da sensibilidade dos dados pessoais tratados e do nível de conhecimento e maturidade que as áreas internas possuem sobre o tema. Por este motivo, é importante que as Concessionárias estudem qual estrutura melhor reflete a sua realidade, não havendo uma configuração única para tanto.

3.9. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação (SI), enquanto ciência que estuda metodologias de proteção à informação, é materializada pelo conjunto de medidas preventivas, detectivas, repressivas e corretivas aptas a proteger a informação (o que inclui, mas não se limita a dados pessoais) contra uma ampla gama de ameaças, a fim de garantir a continuidade do negócio, minimizar riscos e maximizar o retorno sobre investimentos.

Nesse sentido, é necessário primeiramente definir o que seria a informação, para entender o escopo do que está incluso em sua segurança.

5

Informação é um conhecimento inscrito sob a forma escrita, lógica, oral ou audiovisual.

Pode ser resultante do processamento, manipulação e organização de **dados**, de tal forma que represente uma modificação no conhecimento.

Ou pode estar em seu estado original, se referindo de maneira clara e exata a um determinado conhecimento ou orientação.

Com esta premissa, conclui-se que a informação pode estar sob diversos formatos, inclusive sob a forma de dados pessoais. Por isso a SI tem um escopo que abrange dados pessoais, sendo que parte da privacidade e proteção dos dados pessoais, dependem diretamente da implementação de controles de SI. Não à toa o art. 46, da LGPD, exige que os agentes de tratamentos de dados adotem medidas aptas a resguardar os dados pessoais.

Mas a atenção não deve ser destinada somente para dados pessoais, e muito menos somente para o ambiente cibernético. É certo, que majoritariamente, em face da modernidade e tecnologias presentes na sociedade, dados são tratados em ambientes lógicos, mas ainda há dados presentes em arquivos e documentos físicos ou transmitidos oralmente. E para estas situações também deve existir medidas de segurança.

Além disso, destaca-se que não somente dados pessoais são ativos valiosos para as Concessionárias, mas também informações sobre processos, produtos, inovações e estratégias de atuação são igualmente importantes e relevantes para

5 Fonte: https://www.meioemensagem.com.br/assuntos/lei-geral-de-protecao-de-dados. Acesso em 04 de agosto de 2022.

o contexto corporativo, e, assim, também devem ser protegidas contra acessos não autorizados e comprometimento de sua integridade e confidencialidade.

Nesta perspectiva, para que se tenha uma proteção adequada à informação (incluindo dados pessoais), é necessário que os pilares básicos da SI sejam garantidos, quais sejam:

Confidencialidade
garantia de que a informação somente estará acessível para pessoas autorizadas.

Disponibilidade
serviços e informações disponíveis de acordo com as exigências do negócio.

Integridade
garantia de que a informação está correta, atualizada, confiável e não adulterada para utilização.

Com estas considerações, é essencial que a Segurança da Informação seja garantida por estratégias corporativas que compreendam aspectos essenciais relacionados à mudança de cultura, infraestrutura e governança.

No que se refere à cultura, para que ocorra a conscientização do corpo colaborativo, é essencial que exista um plano que promova a educação digital aos profissionais da concessionária, seja mediante promoção de palestras sobre SI, treinamentos profissionais, informativos circulados por e-mail e workshops.

Quais os principais riscos mitigáveis com a educação digital?

i. Vazamento de informações;
ii. Má postura nas redes sociais;
iii. Fraude;
iv. Concorrência desleal;
v. Engenharias sociais;
vi. Uso indevido da marca.

Outro aliado importante da segurança da informação são as medidas de governança que estabelecem responsabilidades e deveres aos colaboradores, determinando como deve ser o modo de operação que considere procedimentos para proteger a informação. As boas práticas referentes à Segurança da Informação serão apresentadas no item 4.9 do presente Guia.

GOVERNANÇA DA INFORMAÇÃO

A Segurança da Informação não somente é valorizada pelas concessionárias por proteger a informação enquanto ativo com valor financeiro, como também visa impedir que incidentes de segurança da informação ocorram. O incidente é caracterizado quando há comprometimento de um dos três pilares da segurança da informação (confidencialidade, integridade e disponibilidade). Ou seja, se algum sistema interno utilizado é comprometido, ou mesmo se um equipamento é infectado por um vírus, divulgando informação confidencial a terceiro não autorizado, são situações consideradas como incidentes.

E incidentes podem ter consequências diversas e cumulativas, por exemplo, interrupção das operações da concessionária, dano à reputação e imagem, dano material por perda de ativos tecnológicos e ações judiciais ou administrativas. O que amplia a necessidade de alinhamento estratégico em Governança da Informação que leve em consideração diferentes aspectos e seja multidisciplinar, pois assim, uma ampla gama de riscos é reduzida.

Destaca-se, ainda, que incidentes de segurança da informação podem envolver dados pessoais, o que pela legislação exige que uma análise de risco seja realizada pelo Encarregado para fins de verificação se o dano ou risco ocasionado é relevante, o que poderá exigir ainda a comunicação à Autoridade Nacional de Proteção de Dados e aos titulares, nos termos do art. 48 da LGPD. Além disso, esta lei exige que o controlador possua um plano de resposta a incidentes (Art. 50, §2º, I, alínea “g”, da LPGD).

Mas o que é um incidente de segurança (violação) de dados pessoais?

Acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Exemplo:

Incidente de violação de dados pessoais pelo comprometimento da integridade dos dados, ocasionando na exclusão, devido à um mal funcionamento no sistema interno de armazenamento das informações.

Este exemplo não necessariamente é causado por uma ameaça externa, podendo ser causado pela presença de um erro (bug) no próprio sistema. Por isso, é importante que se mantenha os sistemas utilizados com as últimas atualizações e patches instalados para as funcionalidades de segurança estarem ativas e evitar problemas técnicos.

Além disso, é essencial que seja mantido backup das informações com intervalo temporal estratégico, para que em caso de problemas como este, não haja interrupção das operações, reduzindo o impacto à concessionária.

Dessa forma, sempre que houver comprometimento da segurança dos dados pessoais, seja por ameaças externas ou vulnerabilidades internas, haverá incidente de dados pessoais. Por isso, que a LGPD determina em seu art. 50, §2º, I, alínea "g", a importância de o Controlador ter estruturado um plano de resposta a incidentes, para que dessa forma, o risco aos titulares e o potencial dano sejam reduzidos.

Este plano de resposta, deve contar com diferentes etapas que abordem: (i) formas de prevenção a incidentes de violação de dados pessoais, (ii) identificação e registro do incidente, (iii) contenção, (iv) restauração, e (v) lições aprendidas. Nesta perspectiva, para cada etapa, diferentes procedimentos devem ser seguidos, construindo uma sistemática que reduza o impacto aos titulares e agentes de tratamento envolvidos, e que cumpra com as exigências legais.

O que fazer quando houver um incidente?

Quando houver um incidente, as seguintes ações devem ocorrer:

Comunicar o **incidente de segurança** ou sua suspeita para Área de TI. A área de TI irá registrar e analisar o incidente, e caso envolva dados pessoais, deverá acionar o Encarregado pelo tratamento de dados da concessionária e o Comitê de Privacidade, se existir.

A área de TI acionará o **plano de respostas** e irá identificar e registrar o incidente, e caso a primeira análise suspeitar ou confirma que o incidente envolve dados pessoais, o **normativo** específico de incidentes de segurança com dados pessoais deverá ser observado.

O Comitê e o Encarregado pelo Tratamento de Dados Pessoais realizarão a análise do incidente, em conjunto com a equipe de TI, e conduzirão a **avaliação do risco ou dano** existente aos titulares.

Se houver risco ou dano relevante aos titulares, a concessionária deve proceder com a **comunicação à ANPD** e aos titulares informando sobre a ocorrência do incidente.

O **Comunicado** deve conter minimamente: (i) a descrição da natureza dos dados pessoais afetados; (ii) as informações sobre os titulares envolvidos; (iii) indicação das medidas de segurança utilizadas para proteção dos dados; (iv) riscos relacionados ao incidente; (v) motivo da demora no caso da comunicação não ter sido imediata e; (vi) medidas que serão adotadas para reverter os prejuízos ou mitigar os efeitos.

Diante da comunicação realizada (quando necessária), a ANPD poderá solicitar a **adoção de providências** como por exemplo: ampla de divulgação do fato em meios de comunicação, e medidas para reverter o prejuízo, que deverão ser atendidas.

Por último, deve haver a **gestão do incidente**, com a continuidade do plano de resposta e suas etapas, sobretudo a restauração e lições aprendidas. Além disso, convém que seja realizado a **gestão de crise**, para lidar com todas as consequências do evento. (jurídico, reputacional, imagem, material).

Importante destacar que, porquanto pendente de regulamentação a definição sobre o prazo e modo conclusivo de comunicação de incidentes à Autoridade Nacional de Proteção de Dados, esta **recomenda que após a ciência do evento adverso e constatando-se a existência de risco relevante, seja ela comunicada com a maior brevidade possível, indicando-se a título indicativo o prazo de 2 dias úteis**, contados da data de conhecimento do incidente[7], reiterando-se que após regulamentação do ente fiscalizador, o prazo a ser obedecido será aquele então estabelecido.

Por isso, convém que o plano de resposta contenha avaliação rigorosa do risco, que se baseie em critérios pré-definidos para proceder com a comunicação, sob pena de atrair fiscalização da autoridade reguladora desnecessariamente.

Contudo, até a determinação pela comunicação, deve-se ter um processo interno no qual busca-se o levantamento das circunstâncias do incidente, com comunicação ao Encarregado pelo Tratamento de Dados Pessoais para avaliação dos riscos atrelados ao evento

Em todos os casos, independentemente de notificação, o incidente deverá ser registrado para fins de gestão, tomada de decisões e até apresentação em eventual fiscalização, inclusive com a justificativa pela decisão de não comunicação.

Boas práticas relacionadas a respostas a incidentes

Ainda que haja robustez no Programa de Governança da Informação das concessionárias, é certo que nenhum sistema de defesa, por mais sofisticado e multidisciplinar que seja, é totalmente seguro. Isto significa, que ainda que seja realizado um grande investimento em segurança da informação e proteção de dados, a concessionária estará suscetível a um incidente de segurança (que pode envolver ou não dados pessoais).

Com esta premissa, é de suma importância que algumas práticas que visam o aperfeiçoamento contínuo do sistema de defesa e que atestam a capacidade efetiva do plano de respostas sejam adotadas, como, por exemplo:

- Simulações de incidentes, para testar a capacidade, efetividade e velocidade de resposta do corpo colaborativo que integram as áreas envolvidas em proceder com os procedimentos formalmente estabelecidos nas etapas de resposta ao incidente;
- Blue team (time azul) x Red team (time vermelho): treinamento técnico da equipe operacional da resposta ao incidente, com esta metodologia, a equipe técnica será separada em 2 (dois) times, red team com a finalidade de

[7] Para comunicar um incidente de segurança para a ANPD, deve-se preencher o formulário eletrônico disponível no site e enviar por meio de Peticionamento Eletrônico – Usuário Externo do SEI, disponível em: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico. Para que seja possível utilizar essa plataforma, deve-se realizar o cadastro, cujo prazo de liberação é de até 3 (três) dias úteis. Ou seja, recomenda-se que o cadastro seja realizado previamente considerando o prazo de liberação e o tempo a menor recomendado pela ANPD.

simular um ataque ao sistema de defesa, e a blue team, com a finalidade de proceder com a defesa deste ataque;

- Treinamentos e conscientização relacionados a diferentes tipos de incidentes, por exemplo, contra ransomwares, phishing, vazamento interno, falha humana, etc.
- Treinamento geral sobre incidentes de segurança, principais causas, e ações necessárias quando de sua ocorrência;
- Adoção de boas práticas em Segurança da Informação como exemplificado no item 4.9 do presente Guia.

Envolvimento das áreas em um incidente

Exemplificamos abaixo algumas das possíveis responsabilidades e contribuições que as áreas podem ter quando da gestão de um incidente de segurança:

Área /Função	Papel em potencial
TI/SI	Investigação e levantamento das circunstâncias do incidente.
Jurídico/Comitê de Privacidade/ Encarregado	Determinação da necessidade de comunicação do incidente à ANPD e/ou titulares, com base no que foi levantado pela equipe técnica.
Encarregado	Orientar quanto aos procedimentos necessários para resposta ao incidente.
RH	Condutor das informações que são repassadas aos empregados.
Financeiro	Verificação dos custos para a solução da questão.
Marketing/Relações públicas	Estabelecimento de narrativa consistente e coerente caso a situação tenha alcance ao grande público, imprensa e autoridades.
Atendimento ao cliente	Centralização das comunicações aos titulares de dados envolvidos, padronizando o atendimento e informações.
Jurídico/Área de Risco	Verificar os titulares atingidos e os prejuízos que sofreram para propor conciliação direta com o titular (Art. 52, §7º, LGPD) evitando eventuais sanções da ANPD.

3.10. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública que, dentre outras atribuições, é responsável por zelar pela proteção de dados pessoais, fiscalizar e aplicar sanções administrativas a quem desrespeitar a LGPD, receber comunicações dos titulares, receber comunicações de incidentes de segurança e estimular o conhecimento sobre proteção de dados pessoais no Brasil.

Criada pela LGPD, em seu art. 55-A, a ANPD era inicialmente um órgão da administração pública federal, integrante da Presidência da República, entretanto, sua natureza era transitória, eis que até dois anos da entrada em vigor da estrutura regimental da ANPD, esta deveria ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial.

Foi o que ocorreu com a edição da Medida Provisória nº 1.124, de 13 de junho de 2022, que alterou o texto do art. 55-A para:

> “Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial, dotada de **autonomia técnica e decisória**, com patrimônio próprio e com sede e foro no Distrito Federal.”

A Medida Provisória deverá ser deliberada pelo Congresso até 25 de agosto de 2022, podendo-se prorrogar o prazo por mais 60 dias.[8]

Acerca de sua estruturação, a ANPD possui a seguinte composição:

- Conselho Diretor (órgão máximo de direção);
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD);
- Corregedoria;
- Ouvidoria;
- Órgão de assessoramento jurídico próprio;
- Procuradoria; e,
- Unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

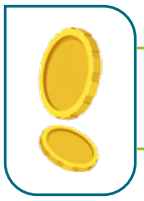
Como mencionado, uma das competências da ANPD é de fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à LGPD, mediante um processo administrativo que assegure o contraditório,

[8] Atualizado em 18/07/2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/06/14/mp-concede-autonomia-de-autarquia-a-autoridade-nacional-de-protecao-de-dados

a ampla defesa e o direito de recurso. Ainda, a LGPD trata em seu art. 55-K da exclusividade da ANPD em aplicar as sanções previstas na legislação, bem como da prevalência de competência, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da Administração Pública.

As sanções administrativas da LGPD podem ser desde uma advertência e publicização da infração, até a penalização pecuniária (com teto de R$ 50 milhões por infração) e a suspensão ou bloqueio da atividade. São elas:

- Advertência
- Publicização da infração



- Multa simples (teto de R$ 50 milhões por infração)
- Multa diária (teto de R$ 50 milhões por infração)

- Bloqueio dos dados pessoais
- Eliminação dos dados pessoais

!

ATENÇÃO:

As sanções impostas pela ANPD não impedem o exercício de direito em processo judicial pelo titular e outras entidades como Ministério Público e Procon, com pedidos de indenização por danos materiais e morais.

Para a imposição de sanções, a LGPD determinou que a ANPD editasse um regulamento para dispor acerca dos processos de fiscalização e sancionador, bem como as metodologias que orientarão o cálculo do valor-base das sanções de multa.

A Resolução CD/ANPD nº 1, de 28 de outubro de 2021[9], aprovou o regulamento do processo de Fiscalização e Administrativo Sancionador. Conforme o art. 15 da regulamentação, a ANPD adotará atividades de monitoramento, orientação e de prevenção no processo de fiscalização e poderá iniciar a atividade repressiva.

As **atividades de monitoramento** destinam-se ao levantamento de informações e dados relevantes para subsidiar a tomada de decisões pela ANPD. Já, as **atividades de orientação** caracterizam-se pela atuação baseada na utilização de métodos e ferramentas que almejam a promover a orientação, a cons-

[9] Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513

cientização e a educação dos agentes de tratamento e dos titulares de dados pessoais. As **atividades preventivas** consistem em uma atuação baseada na construção conjunta de soluções e medidas que visam a reconduzir o agente de tratamento à conformidade ou a evitar ou remediar situações que possam acarretar risco ou danos aos titulares de dados pessoais e a outros agentes de tratamento. Por fim, as **atividades repressivas** verificam-se na atuação coercitiva da ANPD, voltada à interrupção de situações de dano ou risco, à recondução à plena conformidade e à punição dos responsáveis mediante a aplicação das sanções previstas no artigo 52 da LGPD, através do processo administrativo sancionador.

O processo administrativo sancionador é estabelecido pela regulamentação e possui o seguinte fluxo resumido:

4. APLICABILIDADE DA LGPD NO SETOR DE CONCESSÃO DE RODOVIAS

O presente capítulo tem como objetivo demonstrar boas práticas de adequação à LGPD e Governança no setor de concessão de rodovias, de forma a considerar os pontos de dúvidas e atenção trazidos pelas concessionárias, os principais desafios enfrentados pelo setor, bem como práticas setoriais e internacionais.

4.1. REGULAÇÃO SETORIAL

A Lei Geral de Proteção de Dados Pessoais (LGPD) trata-se de uma lei geral, que se aplica a todos os agentes que realizarem o tratamento de dados pessoais independente do setor. Entretanto, existem agentes de tratamento que desenvolvem atividades reguladas e que devem cumprir com obrigações regulatórias, além das obrigações impostas por lei, como é o setor de concessão de rodovias.

Para que as concessionárias estejam em conformidade com as regras de privacidade e proteção de dados pessoais, devem considerar além da LGPD, as regras e diretrizes setoriais.

Dessa forma, apresenta-se, a seguir, as diretrizes e boas práticas implementadas pelo setor quanto a proteção de dados pessoais e segurança da informação:

Agência Nacional de Transportes Terrestres - ANTT:

A ANTT, no que diz respeito ao tratamento de dados pessoais e à segurança da informação, traz diretrizes e esclarece suas principais atividades em dois documentos, quais sejam: o Aviso de Privacidade e a Política de Segurança das Informações e Comunicações.

O **Aviso de Privacidade, disponível** no seguinte link (Aviso de Privacidade - ANTT - https://www.gov.br/antt/pt-br/acesso-a-informacao/protecao-de-dados-pessoais), aborda todos os temas relevantes referentes ao tratamento de dados pessoais realizado pela ANTT, dando transparência e segurança aos Titulares cujos dados estão envolvidos nas atividades da agência. Assim, são elucidadas a finalidade e necessidade dos tratamentos realizados, garantindo-se o compromisso da ANTT com a integridade, confiabilidade e segurança dos dados processados.

Para além disto, no Aviso de Privacidade, ainda são apresentados os pontos principais acerca da Lei Geral de Proteção de Dados – LGPD, como os princípios da lei, os significados dos termos utilizados em seu texto e a definição

de tratamento e dados pessoais. Também são abordados tópicos mais específicos acerca das atividades da agência, como: sua competência; os tipos de dados pessoais tratados; a forma de processamento; informações gerais acerca dos direitos dos titulares e modos de se entrar em contato com o Encarregado da ANTT.

Assim, através deste documento é apresentada, de modo simplificado, como se dá a operação da ANTT com relação ao tratamento de dados pessoais, servindo de exemplo às empresas do setor, para que ajam de acordo com as diretrizes trazidas à luz através deste Aviso.

No tocante à **Política de Segurança das Informações e Comunicações - PoSIC**, publicada na Resolução Nº 5854/2019 (PoSIC - ANTT), esta tem a principal função de servir de guia para as atividades relacionadas a ativos informacionais e de comunicação de todos os agentes, públicos e privados, que executem atividades envolvendo a ANTT, devendo estes a seguirem integralmente para que sejam mantidas as relações com a agência.

Com fins de estabelecer os principais critérios a serem observados pelos sujeitos da PoSIC, em seu texto são abordados, entre outros, os seguintes tópicos: diretrizes gerais para implementação de medidas de segurança cibernética; pontos principais e essenciais para Políticas de Segurança Cibernética; estabelecimento das responsabilidades pela implementação de medidas de segurança cibernética; formas de realizar a notificação de Incidentes Cibernéticos; protocolos para gestão de incidentes; necessidade de registro das atividades relacionadas à Segurança Cibernética; e, por fim, as sanções em caso de descumprimento.

Através dos direcionamentos apresentados no corpo da referida Política, busca-se criar critérios objetivos de segurança das informações para as atividades dos agentes que sejam realizadas em conjunto com a ANTT, de modo a garantir uma adequação mínima dos parceiros da agência, e consequentemente assegurar aos titulares de dados a segurança e o tratamento responsável de seus dados pessoais sob posse da ANTT.

Agência de Transporte do Estado de São Paulo - ARTESP:

A ARTESP, até o momento da realização do presente Guia, não possui documentos oficiais que ofereçam direcionamentos internos ou a terceiros que com ela contratam, acerca de proteção de dados pessoais e segurança da informação. Contudo, através da **Portaria ARTESP Nº 74/2020**, disponível no seguinte link (Portaria nº 74/2020 - http://www.artesp.sp.gov.br/Shared%20Documents/Portarias/74%20-%20Portaria%20LGPD%203%20-%20PROT.%20524.901.pdf), determinou que fosse criado um Grupo de Trabalho

(GT) designado para regulamentar e implementar a LGPD na agência.

Ao referido GT foi designada a função de realizar o "levantamento do fluxo de dados pessoais que a organização possui para fins de elaborar minuta da Política de Proteção de Dados Pessoais e seus Protocolos de atendimento às demandas da LGPD", para além da consequente indicação do Encarregado para a agência.

A execução das determinações apresentadas na Portaria ainda não foi devidamente finalizada, entretanto, já serve como um indicativo para as futuras medidas que serão tomadas pela ARTESP com fins de adequar-se à LGPD e de apresentar um direcionamento às suas parceiras com relação ao modo de implementação da lei que entende ser mais efetivo para as empresas do setor.

Confederação Nacional do Transporte - CNT:

A CNT possui em seu Portal, para além da Política de Privacidade, que descreve como ocorre o tratamento de dados pessoais internamente na Organização, dois documentos com a finalidade de servirem como guias para a adequação à LGPD das empresas do setor de transporte. Os documentos são o Guia de Boas Práticas para o Setor de Transporte, e LGPD no Setor de Transporte.

Primeiramente, o **Guia de Boas Práticas**, disponível no seguinte link (Guia de Boas Práticas para o Setor de Transporte - https://publicador.sestsenat.org.br/arquivos/b37861f6-e632-45d7-89ca-e8cdbca3d267.pdf), apresenta considerações iniciais acerca da LGPD, expondo os seus principais conceitos, aplicações e bases principiológicas, de modo a assegurar um conhecimento mínimo da lei para os interessados na adequação de suas empresas.

Após as explicações iniciais sobre a LGPD, o guia passa a abordar os principais protocolos úteis na prática da implementação de uma estrutura de governança de proteção de dados nas empresas do setor de transporte, dividindo os tópicos em Protocolos Gerais e Protocolos Especiais. Nos protocolos gerais, são abordados temas como transporte de passageiros, tratamento de dados de empregados e prestadores de serviço, segurança da informação, direito dos titulares, entre outros. Já no que diz respeito aos protocolos especiais, observa-se que o que o exposto refere-se a três sensíveis tópicos para o setor em comento, abordando as melhores práticas a serem aplicadas em situações que envolvam: cartões de transporte; imagem, biometria e reconhecimento facial; e exames toxicológicos.

O segundo importante documento da CNT que direciona as atividades das empresas do setor de transporte é o "**LGPD no Setor de Transporte**", disponível no seguinte link (LGPD no Setor de Transporte - https://publicador.sestsenat.org.br/arquivos/2b22a889-cc41-4315-9a0b-09fb252dcf6e.pdf),

que dá orientações para a implementação da LGPD na estrutura interna das empresas. Este documento apresenta uma abordagem mais superficial acerca da LGPD quando comparado com o Guia previamente tratado, trazendo em seu texto os principais conceitos da lei e as hipóteses em que suas normas são aplicáveis em casos concretos.

O referido documento também expõe um rápido passo a passo para a adequação das empresas do setor aos ditames da LGPD, explicando acerca da importância de todas as principais etapas do processo de implementação da lei, desde o mapeamento das atividades de tratamento de dados pessoais até os treinamentos e mudanças na cultura da empresa. Neste mesmo tocante, também apresenta um curto rol de boas práticas e alguns exemplos práticos para didaticamente ensinar aos interessados como melhor agirem pensando na completa obediência à LGPD.

Por fim, dentro de um contexto interno da CNT, em seu Portal também é disponibilizada sua **Política de Privacidade** (link para a Política de Privacidade - https://publicador.sestsenat.org.br/arquivos/ce66f060-8d92-46fb-a5b9-d95ec86e4b98.pdf), que tem "por finalidade demonstrar o compromisso do Sistema CNT com a privacidade e a proteção dos dados pessoais coletados de seus empregados, terceiros, parceiros, fornecedores, e principalmente de seus usuários e contribuintes".

Neste último documento, são abordados todos os principais pontos com fins de dar transparência ao sistema interno de governança de dados pessoais aplicado no Sistema CNT, englobando questões relacionadas à coleta, armazenamento, finalidades do tratamento, compartilhamentos e transferências internacionais, término do tratamento e formas de exercício dos direitos dos titulares.

Deste modo, o Sistema CNT apresenta uma estrutura mínima necessária às políticas de privacidade das empresas do setor de transportes, para que o documento cumpra sua função de transparência para com a sociedade e órgãos fiscalizatórios.

4.2. MAPEAMENTO REGULATÓRIO/MARCO NORMATIVO

Normas Gerais Federais

- **PORTARIA - GM Nº 235, DE 28 MARÇO DE 2018:** Institui a Política Nacional de Transportes e estabelece princípios, objetivos, diretrizes e instrumentos para o setor de transportes.

- **LEI Nº 8.987, DE 13 DE FEVEREIRO DE 1995:** Dispõe sobre o regime de concessão e permissão da prestação de serviços públicos previsto no art. 175 da Constituição Federal, e dá outras providências.

Resoluções ANTT

- **RESOLUÇÃO 2.064 DE 2007 DA ANTT:** Dispõe sobre a utilização de sistema de monitoramento de tráfego por meio de Circuito Fechado de Televisão - CFTV em concessões rodoviárias federais reguladas pela ANTT.

- **RESOLUÇÃO 3.576 DE 2010 DA ANTT:** Dispõe sobre as especificações e preços dos Sistemas ITS (Intelligent Transportation Systems) de Sensoriamento de Tráfego Veicular; de Painéis de Mensagens Variáveis - Fixos; de Painéis de Mensagens Variáveis - Móveis; de Sensoriamento Meteorológico; de Circuito Fechado de TV - CFTV e de Detecção de Altura, a serem adotados nas rodovias federais concedidas, reguladas pela ANTT.

- **RESOLUÇÃO Nº 5.950, DE 20 DE JULHO DE 2021:** Aprova o Regulamento das Concessões Rodoviárias.

- **RESOLUÇÃO Nº 675, DE 4 DE AGOSTO DE 2004:** Dispõe sobre as revisões ordinárias, extraordinárias e quinquenais do equilíbrio econômico-financeiro dos contratos das concessões rodoviárias federais.

- **RESOLUÇÃO Nº 5.927, DE 2 DE MARÇO DE 2021:** Estabelece as regras e procedimentos a serem observados pelas concessionárias para análise de transferência de concessão ou do controle societário da concessionária, de transformações societárias decorrentes de cisão, fusão, incorporação e formação de consórcio de empresas concessionárias, de pulverização do capital social da concessionária, de aquisição originária de controle societário e de celebração, alteração ou extinção de Acordo de Acionistas.

- **PORTARIA Nº 227, DE 21 DE MAIO DE 2020:** Dispõe sobre o estudo e a implementação de melhorias regulatórias e de governança relacionadas aos contratos de concessão de infraestruturas de transporte terrestre, com o intuito de propiciar maior transparência, celeridade e previsibilidade.

- **RESOLUÇÃO Nº 5.857, DE 12 DE NOVEMBRO DE 2019:** Regulamenta a comprovação de Regularidade Fiscal das Concessionárias do Serviço Público de Exploração da Infraestrutura Rodoviária Federal e das Concessionárias do Serviço Público de Transporte Ferroviário de Cargas e Passageiros, reguladas pela ANTT.

- **RESOLUÇÃO Nº 3.514, DE 12 DE MAIO DE 2010:** Aprova o Regulamento que estabelece procedimentos para a dispensa da exigência de manutenção de bloco de controle majoritário identificado na organização societária de empresas concessionárias de serviços de transportes terrestres, facultando a adoção de nova estrutura de governança corporativa.

- **RESOLUÇÃO Nº 2.495, DE 13 DE DEZEMBRO DE 2007:** Determina que as concessionárias do Serviço Público de Exploração da Infraestrutura Rodoviária Federal e as concessionárias do Serviço Público de Transporte Ferroviário de Cargas e Passageiros ou exploração da infraestrutura ferroviária prestem informações trimestrais e anuais, e dá outras providências.

- **PORTARIA Nº 90, DE 9 DE MARÇO DE 2022:** Disciplina o funcionamento das comissões tripartites de rodovia concedida no âmbito dos contratos de concessão de exploração de infraestrutura rodoviária sob competência da Agência Nacional de Transportes Terrestres, nos termos da Resolução nº 5.938, de 4 de maio de 2021.

- **PORTARIA Nº 426, DE 20 DE DEZEMBRO DE 2021:** Disciplina os sistemas e os procedimentos para processamento de dados pela Superintendência de Infraestrutura Rodoviária relativos às informações apresentadas pelas concessionárias no âmbito dos contratos de concessão de exploração de infraestrutura rodoviária sob gestão da Agência Nacional de Transportes Terrestres.

Resoluções CONTRAN

- **RESOLUÇÃO Nº 471 DE 18 DE DEZEMBRO DE 2013:** Regulamenta a fiscalização de trânsito por intermédio de videomonitoramento em estradas e

rodovias, nos termos do § 2º do artigo 280 do Código de Trânsito Brasileiro.

- **RESOLUÇÃO Nº 774, DE 28 DE MARÇO DE 2019:** Revoga a Resolução CONTRAN nº 709, de 25 de outubro de 2017, que dispõe sobre a publicação na internet dos nomes e códigos dos agentes e autoridades de trânsito, bem como os convênios de fiscalização de trânsito celebrados pelos órgãos e entidades executivos de trânsito.

- **RESOLUÇÃO CONTRAN Nº 909, DE 28 DE MARÇO DE 2022:** Consolida normas de fiscalização de trânsito por intermédio de videomonitoramento, nos termos do § 2º do art. 280 do Código de Trânsito Brasileiro (CTB).

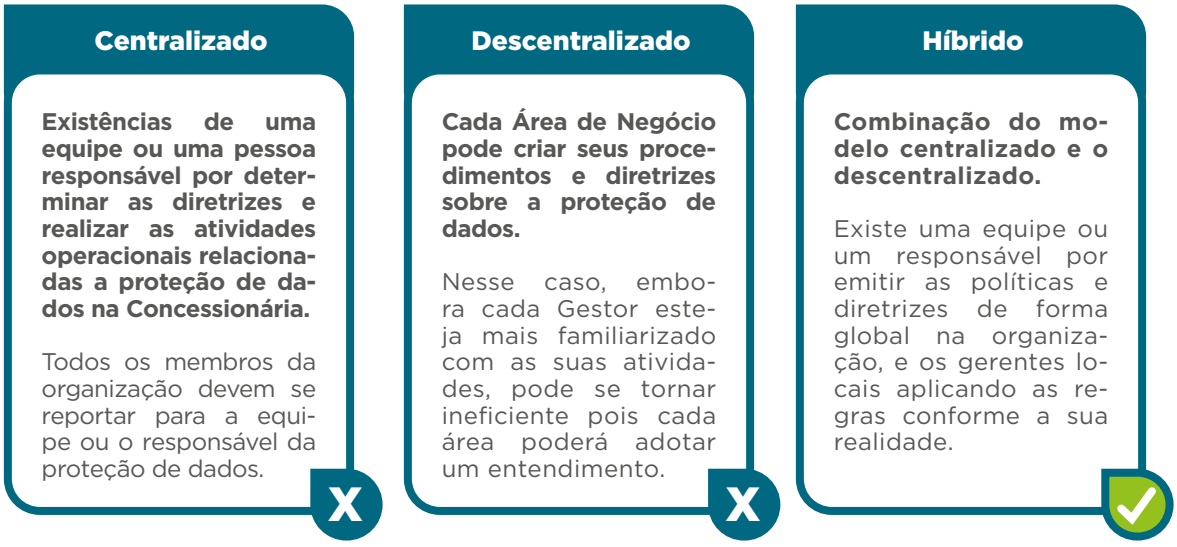
4.3. SETOR INTERNACIONAL

Durante as pesquisas realizadas para este Guia, foram investigadas as melhores práticas internacionais relacionadas à proteção de dados pessoais no setor de concessão de rodovias, e constatou-se a indisponibilidade de informações relativas ao tema, especialmente no contexto europeu e americano, sendo consideradas as práticas adotadas no Brasil como as mais avançadas no mercado, tendo em vista este setor ter maior robustez no país.

4.4. DA ESTRUTURAÇÃO DE UM PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS

O estabelecimento de um programa de governança em privacidade de proteção de dados nas Concessionárias, além de ser uma boa prática prevista no art. 50 da LGPD, trata-se de uma forma de gerir e implementar todos os aspectos legais e regulatórios relacionados à temática.

Para que a organização estruture o programa de governança, faz-se necessário, estabelecer inicialmente, o modelo de governança a ser adotado: centralizado, descentralizado ou híbrido.



A materialização do modelo de governança em privacidade deve refletir a realidade de cada organização, não havendo, portanto, o mais correto. Cada modelo traz vantagens e desvantagens, devendo ser avaliado para melhor atender as necessidades quanto à proteção dos dados pessoais.

No modelo centralizado, todos os membros da organização devem se reportar para a equipe ou responsável pela proteção de dados pessoais. Tal modelo possui desvantagens ao passo que para sua estruturação, faz-se necessário uma equipe muito grande e multidisciplinar para a realização das atividades, o que demanda alto investimento na área e ausência de segregação de função.

No modelo descentralizado, embora cada gestor esteja mais familiarizado com suas atividades, pode se tornar ineficiente pois cada área poderá adotar um entendimento. Nesse sentido, cada Área de Negócio pode criar seus procedimentos e diretrizes sobre proteção de dados, o que pode trazer, o que exige que gestores possuam expertise e maturidade sobre o tema, o que igualmente demanda alto in-

vestimento pela organização, para a capacitação de todos.

Dessa forma, o modelo mais indicado para estruturar o programa de governança – **o que não se confunde com a materialização, que leva em conta cada estrutura empresarial** - é o híbrido, pois mediante a combinação de abordagens centralizadas e descentralizadas, permite com que a organização alcance os resultados esperados, com abrangência em todos os seus níveis, uniformização de entendimento e adequação à realidade e necessidade da área.

Para que a estruturação do programa de governança em privacidade e proteção de dados, no modelo híbrido, funcione recomenda-se a criação de um comitê de privacidade e segurança da informação, a ser constituído dentro da organização.

DA PRIVACIDADE COMO PADRÃO DE ATUAÇÃO

A implementação do programa de governança em privacidade de proteção de dados nas Concessionárias deve ainda considerar a aplicação de diretrizes de operacionalização para toda cadeia de serviços, produtos, ações ou equivalente, a partir da adoção da privacidade como um padrão de segurança, ao passo que se orientem pelos seguintes conceitos:

- **Privacy by Design:** Framework que visa incorporar a privacidade e a proteção de dados pessoais desde a concepção de todos os projetos desenvolvidos, neste caso, pelas Concessionárias, e que deve considerar a observância de 7 princípios (Proativo, e não reativo; preventivo, e não corretivo; Privacidade como padrão geral; Privacidade incorporada ao design; Funcionalidade total; Segurança de ponta a ponta; Visibilidade e transparência; Respeito pela privacidade do usuário como ente central);

- **Privacy by Default:** Conceito que representa a ideia de aplicação da privacidade como padrão, indicando assim a necessidade de adotar-se esta e a proteção de dados pessoais em todos os processos e atividades desenvolvidos pelas Concessionárias, mesmo após o seu desenvolvimento. Compreende a necessidade de aplicação e verificação das medidas de segurança, técnicas e organizacionais, para garantir a privacidade como essência de todas as operações realizadas;

- **Security by Design:** Envolve pensar também a segurança durante o desenvolvimento de novos processos, produtos ou serviços, especialmente aplicando testes e outros meios de verificação que permitam garantir que o novo procedimento possui fatores de aplicação que denotam a sua aderência a padrões necessários de segurança. Assim, há de se pensar em toda estrutura de análise de vulnerabilidades e avalição de riscos, valendo-se, inclusive, das diretrizes aplicadas à segurança da informação.

COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O Comitê poderá ser instituído internamente na Concessionária, para que os assuntos relacionados à privacidade, proteção de dados pessoais e segurança da informação sejam centralizados. O papel do Comitê reside no apoio ao cumprimento da LGPD, boas práticas de segurança da informação e tratamento de dados pessoais pela Concessionária, bem como no auxílio para tomada de decisão quanto aos procedimentos a serem adotados em situações concretas pertinentes ao tema. São as responsabilidades do Comitê:

- Rever periodicamente a política de governança de dados pessoais e demais normas relacionadas, sugerindo possíveis alterações, aperfeiçoamentos, esclarecendo dúvidas e deliberando sobre questões não contempladas na política e em normas relacionadas.
- Propor e acompanhar planos de ação para aplicação das políticas e campanhas de conscientização junto aos colaboradores, parceiros e fornecedores da Concessionária.
- Discutir as sanções e penalidades ao descumprimento das normas referentes à política de governança de dados pessoais.
- Aprovar e revisar periodicamente o plano do programa de governança em privacidade e proteção de dados, a partir das definições estratégicas.
- Aprovar as campanhas de conscientização e manutenção das políticas relacionadas à privacidade e proteção de dados.
- Estabelecer e direcionar as iniciativas relacionadas a privacidade e proteção de dados pessoais na Concessionária, de forma a estabelecer uma relação consistente entre as estratégias de negócios, tecnologia da informação, controles de segurança da informação e privacidade.
- Apoiar na definição e aprovar os indicadores e metas relacionadas à privacidade, bem como analisar os resultados de auditoria de ativos da informação (pessoas, processos e tecnologia).
- Apoiar a implementação de soluções para tratamento e mitigação de riscos no tratamento de dados pessoais.

Definida a forma de estruturação do programa de governança em privacidade e proteção de dados, passa-se à organização das ações e medidas que devem ser executadas para que o programa seja devidamente implementado na Concessionária. Geralmente, o programa de governança é dividido em quatro fases:

FASE DE PREPARAÇÃO

A fase de preparação consiste na realização de uma análise de leis e regulamentações de privacidade aplicáveis à concessionária, o impacto no negócio, bem como a definição de plano de ação de adequação.

Para que a Concessionária consiga avaliar todas as legislações e regulamentações aplicáveis às suas atividades, recomenda-se que seja realizado um **mapeamento** para consolidação de todas as atividades de tratamento de dados pessoais e a devida atribuição das respectivas bases legais afim de legitimar os tratamentos realizados. A ferramenta desse mapeamento é o Registro das Operações de Tratamento de Dados Pessoai, também conhecido ROPA (Records of Processing Activities), já abordado no item 3.4 do presente Guia.

Ademais, considerando o modelo de estruturação do programa definido, a Concessionária deve **definir os papéis e responsabilidades** dos Colaboradores que irão apoiar a estrutura e manutenção do programa.

Não obstante, recomenda-se a elaboração de uma **Política de Governança em Proteção de Dados** que defina a estratégia e os objetivos de privacidade da Concessionária e as regras e diretrizes para o correto tratamento de dados pessoais, em conformidade com a LGPD.

FASE DE ORGANIZAÇÃO

A fase de organização verifica-se na elaboração de estruturas e mecanismos operacionais para que o programa possa ser devidamente executado.

Assim, o primeiro ponto é a **nomeação de um Encarregado pelo Tratamento de Dados Pessoais**, que possui como principal responsabilidade ser o ponto de contato entre a Concessionária, o titular e a Autoridade Nacional de Proteção de Dados (ANPD). As funções e responsabilidades do Encarregado foram apresentadas no item 3.8 do presente Guia.

Nessa fase, ainda é avaliada pela Concessionária acerca da necessidade de contratação de uma ferramenta que automatize a gestão do programa de governança em privacidade e proteção de dados.

FASE DE IMPLEMENTAÇÃO

A fase de implementação consiste no desenvolvimento e implementação de métodos e controles, com a finalidade de estabelecer as boas práticas de privacidade e segurança dentro da organização.

Para isso, faz-se necessária a edição e publicação de políticas, normas e procedimentos internos que sustentam o programa e auxiliam na definição de controles a serem adotados para garantir a privacidade e proteção de dados.

A seguir listamos alguns tópicos que devem ser tratados na estrutura documental interna do programa:

- **Avaliações de Impacto à Privacidade:** A concessionária deve estabelecer diretrizes sobre a implementação de procedimentos e medidas de segurança técnicas e organizacionais, desde o início de novos projetos, processos, implementação de nossos sistemas e tecnologias, mudanças organizacionais ou demais iniciativas envolvendo o tratamento de dados pessoais, de forma a identificar o impacto do tratamento na privacidade dos titulares e adotar medidas para mitigação do impacto e eventuais riscos.
- **Avaliação do Legítimo Interesse como Hipótese de Tratamento de Dados Pessoais:** Quando o tratamento dos dados pessoais for enquadrado como legítimo interesse (art.7º, inciso IX da LGPD), recomenda-se que seja realizada uma avaliação do legítimo interesse, de forma que seja realizado um teste de balanceamento entre os interesses da concessionária e os direitos e garantias dos titulares, para garantir que os primeiros não se sobressaiam aos últimos, bem como para identificar possibilidades de minimização do tratamento de dados pessoais.
- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** O RIPD trata-se de um documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação dos riscos. Recomenda-se que o RIPD seja então realizado quando houver o tratamento de dados pessoais que se enquadrem neste perfil (riscos às liberdades civis e aos direitos fundamentais dos Titulares de dados pessoais), observando-se ainda as orientações do Enunciado 679 da IX Jornada de Direito Civil do Conselho da Justiça Federal, quando observado o tratamento de alto risco.
- **Direitos dos Titulares:** Os direitos dos titulares, já mencionados no presente Guia no item 3.6, devem ser observados pela concessionária. Dessa forma, recomenda-se o estabelecimento de regras e diretrizes para o atendimento das requisições dos titulares.
- **Avaliação da Proteção de Dados em Terceiros:** A avaliação de terceiros, como due diligence de contratação, é extretamente importante pois considera e avalia o terceiro quanto à conformidade com a LGPD, o que mitiga risco no tratamento de dados pessoais. Assim, a concessionária deve estabelecer os procedimentos de avaliação do nível de proteção de dados pessoais nos terceiros que realizam o tratamento de Dados Pessoais sob a responsabilidade da concessionária.

- **Segurança da Informação:** O programa de governança em privacidade e proteção de dados deve prever, em sua estruturação documental interna, diretrizes sobre a preservação da confidencialidade, integridade e disponibilidades das informações, incluindo dados pessoais, de propriedade ou sob a responsabilidade da concessionária.
- **Gestão de Incidentes de Violação de Dados Pessoais:** A concessionária deve estabelecer os procedimentos para identificação, registro e contenção de incidentes envolvendo Violação de dados pessoais, assim como as diretrizes para análise da necessidade de notificações em relação ao incidente, caso o risco ou dano seja relevante.
- **Plano de Treinamentos e Ações de Conscientização:** Como parte do programa de governança em privacidade e proteção de dados, recomenda-se a elaboração de um plano de treinamento e ações de conscientização, para que a cultura de privacidade e proteção de dados pessoais seja difundida dentro da organização.

FASE DE GOVERNANÇA, AVALIAÇÃO E MELHORIA

A fase de governança, avaliação e melhoria verifica-se no estabelecimento de mecanismos para avaliação e melhoria contínua dos aspectos relacionados à privacidade e proteção de dados pessoais na Concessionária.

Aqui, ressalta-se a necessidade de que toda a estrutura documental interna do programa seja devidamente disponibilizada a todos os colaboradores, bem como que seja atualizada de forma periódica.

Não obstante, a concessionária deverá definir e divulgar um canal de contato com o Encarregado para que os titulares possam entrar em contato e exercer seus direitos, para que a Autoridade Nacional de Proteção de Dados (ANPD) possa entrar em contato, assim como para que os colaboradores possam solicitar orientações e tirar dúvidas acerca do programa.

Não obstante, a Concessionária deve desenvolver um plano de monitoramento e revisão periódica do programa, definindo indicadores, métricas e controles para verificar o cumprimento da estrutura documental interna do programa, a adesão dos colaboradores e o nível de adequação da concessionária à LGPD.

Atrelado ao monitoramento, recomenda-se que sejam realizadas auditorias para avaliação periódica da eficácia do programa estabelecido, de forma medir a adequação ou não à estrutura documental interna do programa e seus controles.

Por fim, destaca-se a necessidade do monitoramento legislativo e das publicações da Autoridade Nacional de Proteção de Dados (ANPD), a fim de identificar mudanças que impactam no programa estabelecido.

4.5. TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS: POLÍTICA DE PRIVACIDADE E POLÍTICA DE COOKIES

A transparência no Tratamento de Dados Pessoais é um princípio de extrema importância trazido pela **LGPD** e que deve ser observado para que a Concessionária atinja conformidade com a legislação.

> VI – 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.

Conforme visto no item 3.1 deste Guia, o Titular está no centro da proteção legislativa e deve ter seus direitos e garantias fundamentais observados pelos Agentes de Tratamento. Para somar com tal afirmativa, destaca-se que a lei traz como um de seus fundamentos a autodeterminação informativa (Art. 2º, inciso II), entendida como o poder de decisão do Titular a respeito do Tratamento de seus Dados Pessoais. Ou seja, o Titular tem domínio sobre os seus Dados Pessoais, ainda que o Tratamento seja legítimo.

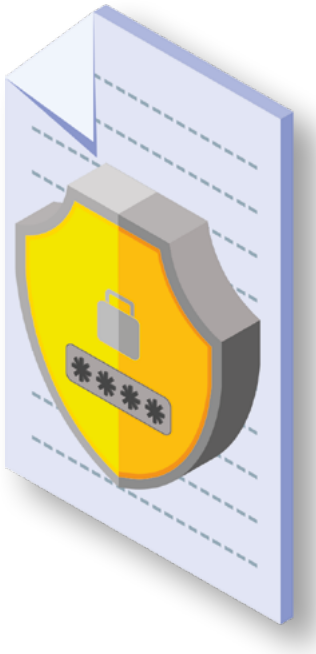
Dessa forma, o princípio da transparência ganha forma e importância na medida em que prevê informações suficientes a respeito do Tratamento dos Dados Pessoais, para que o Titular possa se autodeterminar em relação a eles, seja mediante a ciência da forma e meios de Tratamento seja exercendo um de seus direitos, mencionados no item 3.6 deste Guia.

Embora fique claro que os Agentes de Tratamento devem fornecer aos Titulares informações claras e precisas a respeito do Tratamento, a LGPD não estabelece um rol de requisitos e forma determinada para a efetivação desse princípio.

Assim, como boa prática de privacidade e proteção de dados pessoais, recomenda-se a concessão de transparência ao Titular quanto ao Tratamento de seus Dados Pessoais através de uma Política de Privacidade.

Importa destacar que a Política de Privacidade deve, preferencialmente, ser fornecida antes da coleta dos Dados Pessoais e pelo mesmo meio do Tratamento. Ou seja, se os dados são coletados através de um site, a política deve ser disponibilizada no respectivo site.

POLÍTICA DE PRIVACIDADE



A Política de Privacidade é o documento utilizado para explicar como os Dados Pessoais do Titular são tratados. É por meio dela que as Concessionárias podem cumprir com todas as responsabilidades de transparência e livre acesso à informação impostas pela LGPD.

Dentre os elementos que a Política de Privacidade deve conter, destacamos alguns:

- Identificação e contato da Concessionária (Controladora);
- Quais Dados Pessoais são tratados;
- Como os Dados Pessoais são tratados;
- O motivo pelo qual os Dados Pessoais são tratados (finalidade);
- Se há compartilhamento de Dados Pessoais;
- Se há transferência internacional de Dados Pessoais;
- Quais as práticas de segurança são adotadas pela Concessionária para proteger os Dados Pessoais;
- Como o Titular poderá controlar seus Dados Pessoais (exercício de direitos);
- A forma e a duração do Tratamento dos Dados Pessoais; e
- Identificação e contato do Encarregado.

POLÍTICA DE COOKIES

Salienta-se, igualmente, a importância da Política de Cookies, uma vez que os cookies são pequenos arquivos enviados pelos sites, salvos no dispositivo, que armazenam as suas preferências de navegação e outras informações, as quais podem identificar o Titular, com a finalidade de personalizar a navegação de acordo com o perfil do usuário.

Ainda que a LGPD não trate diretamente de cookies, é inegável que, as definições se mostram compatíveis em sua essência, já que podem identificar o Titular.

Como boas práticas, tem-se levado em consideração manifestações da própria ANPD, que emitiu recentemente um ofício técnico apresentando as

recomendações quanto a adequação de Política de Cookies, bem como publicou, na sequência, Guia orientativo de cookies e proteção de dados pessoais, sendo assim imperativo:

- Identificar as bases legais utilizadas, de acordo com cada finalidade e categoria de cookie, sendo o consentimento a principal base legal a ser utilizada, exceto quando da utilização de cookies estritamente necessários, que podem se baseados no legítimo interesse;
- Classificar os cookies em categorias utilizadas;
- Permitir a obtenção do consentimento específico de acordo com as categorias identificadas; e
- Disponibilizar um botão de fácil visualização, que permita que o titular rejeite todos os cookies não necessários.

Além disso, é também boa prática a disponibilização do **banner de cookies** quando do acesso às plataformas digitais pelo Titular, havendo o desativamento de cookies baseados no consentimento por padrão (opt-in), bem como a disponibilização de um botão de fácil visualização, que permita rejeitar todos os cookies não necessários.

4.6. AGENTES DE TRATAMENTO

Neste tópico serão conceituados os Agentes de Tratamentos previstos na LGPD, os quais já foram mencionados, inclusive, no item 3.2 deste Guia. Ressaltamos que é de extrema importância que os conceitos estejam claros para que, a partir deste entendimento, seja analisado o enquadramento das Concessionárias nas relações que firmarem com o Poder Público, com os prestadores de serviços e com os parceiros comerciais, por exemplo.

A LGPD possui duas figuras como Agentes de Tratamento (art. 5º, VI e VII) e adota as seguintes definições:

1. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
2. **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

As obrigações das partes envolvidas em um Tratamento de Dados Pessoais serão definidas e dispostas de acordo com o papel exercido por cada uma no Tratamento.

A complexidade e o dinamismo das relações jurídicas e operacionais existentes no mercado atual impedem que as relações entre Agentes de Tratamento se restrinjam a interações exclusivamente entre Controladores e Operadores. Vejamos exemplos a seguir:

1. Se a empresa "A" contrata "B", um colaborador pessoa jurídica para prestar serviço especializado em tecnologia da informação em seus ambientes, "B" está em uma posição de Operador de "A", pois prestará o serviço em nome e para "A", utilizando de sua expertise, mas acatando as diretrizes de "A" quanto ao tratamento dos dados pessoais **(Controlador ➡ Operador)**;

2. Se "A" contrata um serviço de headhunting executivo de "B", tanto "B" quanto "A" estão em uma posição de Controladores, pois, enquanto "A" tem o interesse final na contratação do executivo e irá determinar o perfil da vaga, "B" tem o interesse em preencher aquela vaga e irá elaborar relatórios e pareceres sobre os candidatos, tomando as decisões de quais titulares se enquadram no que "A" está buscando **(Controlador ➡ Controlador: Controladoria Conjunta)**;

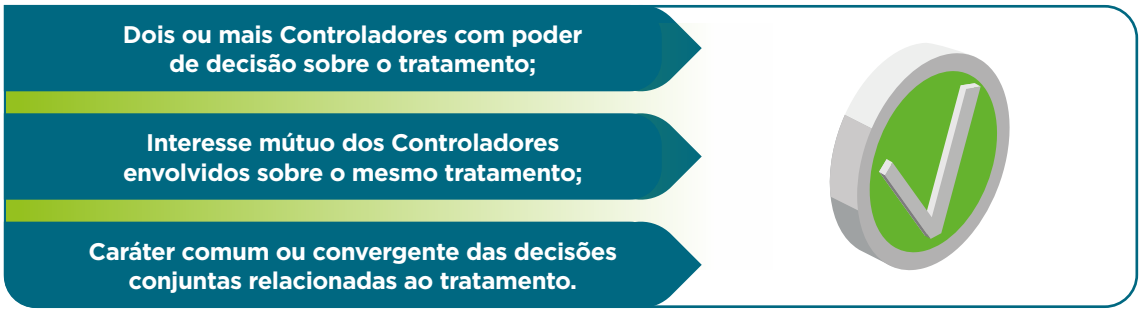
3. Se "A" e "B" tratam dados abertos do governo, cada um para suas finalidades específicas, "A" e "B" são Controladores, mas as operações tratamentos são realizadas de forma independente por cada Controlador, para atingir finalidades próprias de cada um **(Controlador ≠ Controlador: Controladoria Singular)**.

Verifica-se que, apesar da LGPD trazer como Agentes de Tratamento apenas as figuras do Controlador e do Operador, há situações em que duas ou mais partes envolvidas na operação sejam Controladoras em relação aos Dados Pessoais tratados.

As Controladoras decidem sobre o Tratamento de Dados Pessoais, assumindo obrigações perante os Titulares e se tornando responsáveis sobre as atividades que lhes couberem. Nessas hipóteses, a relação poderá ser enquadrada dentro de duas possibilidades: **Controladoria Conjunta ou Controladoria Singular**.

A **Controladoria Conjunta** está conceituada no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado ("Guia Orientativo"), publicado pela Autoridade Nacional de Proteção de Dados ("ANPD"), como sendo "a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo

que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD"[10]. Ou seja, para que uma relação de Controladoria Conjunta possa ser identificada, é necessário que se observem três critérios:



Quanto às decisões conjuntas tomadas pelas Controladoras, conforme indicado pelo terceiro item da checklist acima, elas poderão se revelar de duas formas possíveis:

1. **Decisões comuns**, quando as intenções com o Tratamento forem as mesmas para os Controladores envolvidos; ou

2. **Decisões convergentes**, quando as decisões forem distintas, mas se complementem de tal forma que o Tratamento não seria possível sem a participação de todos os Controladores envolvidos.

Nesse cenário em que todos os requisitos sejam preenchidos, **a relação entre Controladores Conjuntos será regulada por meio de acordo**, podendo este ser o próprio instrumento contratual que firma a relação entre as partes, mediante a inclusão de clausulado específico, ou um acordo específico de Tratamento de Dados Pessoais para aquela determinada operação.

No mais, é imprescindível ressaltar que a própria LGPD estabelece que, perante o Titular, a responsabilidade entre os Controladores Conjuntos é solidária, nos termos do seu art. 42, §1º, II.

Verifica-se, ainda, que somente mediante a análise específica da relação entre as partes é que se torna possível a identificação da existência da Controladoria Conjunta. **Caso, no decorrer da análise, a Concessionária perceba que um ou mais critérios necessários para a caracterização de Controladoria Conjunta não existam, a relação existente entre as partes será a de Controladoria Singular, ou seja, dois Controladores independentes**.

Portanto, a **Controladoria Singular é residual**, ou seja, existirá nos cená-

[10] Guia Orientativo sobre Agentes de Tratamento disponível no link: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

rios nos quais uma ou mais condicionantes apresentadas na checklist acima não existirem. Nesse cenário, **as operações de Tratamentos são realizadas de forma independente por cada Controlador, para atingir finalidades próprias de cada um**.

A seguir serão apresentadas as recomendações que devem ser observadas pelas Concessionárias ao firmarem contratos com o Poder Público, com prestadores de serviços e com parceiros comerciais, a fim de indicar o posicionamento, os direitos, as responsabilidades e as obrigações de cada parte na operação enquanto Agentes de Tratamento, nos termos da LGPD.

4.7. OBRIGAÇÕES CONTRATUAIS E RESPONSABILIDADES

A adequação contratual é de suma importância para a efetivação das diretrizes expostas neste Guia. Isto porque, por meio de instrumento elaborado entre as partes, serão estipuladas as devidas obrigações e responsabilidades assumidas por cada parte, sem prejuízo das obrigações previstas na legislação aplicável.

Importante observar que dentre os fatores a serem considerados para uma revisão contratual no que tange à proteção de dados pessoais, deve-se considerar que temas correlatos interferem na relação que envolve a obrigação ou desobrigação do tratamento. Assim, ao constatar-se, por exemplo, a existência de riscos trabalhistas evidentes, dada a relação eventual de subcontratação, devem as Concessionárias abordar a possibilidade de manutenção desses dados, ou ajustes com os terceiros para que o façam sob condições contratuais. O mesmo se diz das obrigações tributárias que podem judicialmente recair, mesmo que indiretamente, sobre as Concessionárias.

Portanto, recomenda-se que, além do contrato de concessão de sistema de rodovias, os demais contratos firmados com parceiros comerciais, fornecedores e prestadores de serviços sejam adequados à LGPD de modo que reflitam as obrigações e responsabilidades de cada parte como Agentes de Tratamento.

Desta forma, ao analisar cada contrato, recomendamos as seguintes diretrizes:

1. Identificar a posição de cada parte como Agente de Tratamento na operação (Controlador ou Operador).
2. Identificar a operação de Tratamento realizada e suas características: volume, natureza dos dados, finalidade de tratamento etc.
3. Negociar as cláusulas envolvendo proteção de Dados Pessoais, atribuindo responsabilidades, limitações de atuação, direito de regresso, multas etc.
4. Formalizar o contrato entre as partes.

A seguir serão propostas algumas perguntas, a fim de auxiliar na análise do posicionamento da Concessionária como Agente de Tratamento:

1. A Concessionária decide tratar Dados Pessoais?
2. A Concessionária decide quais Dados Pessoais tratar e de quais Titulares?
3. A Concessionária está submetida a uma obrigação legal para tratar os Dados Pessoais?
4. A Concessionária determina a base legal de operação de Tratamento?
5. Os Titulares são colaboradores ou clientes da Concessionária (ou seja, possui relação contratual?)

Se a resposta às perguntas acima for sim, então a Concessionária assume a **posição de Controladora**.

Por outro lado, **se a resposta às perguntas acima for não**, recomenda-se as seguintes perguntas:

1. A Concessionária segue instruções/diretrizes de outras partes para o Tratamento?
2. A Concessionária coletou Dados Pessoais a mando de outra parte?
3. A Concessionária deve devolver ou excluir os Dados Pessoais ao término do contrato/operação de Tratamento?

Se a resposta às perguntas acima for sim, então a Concessionária assume a **posição de Operadora**.

4.8. TEMPO DE GUARDA

O princípio de necessidade traz uma questão importante referente à limitação de armazenamento. Essa questão não trata de limitação física ou de capacidade de armazenamento, mas sim do tempo, ou seja, do período em que os Dados Pessoais ficarão armazenados.

Segunda essa determinação, os Dados Pessoais poderão ser armazenados enquanto perdurar as finalidades atreladas ao Tratamento ou até o momento em que haja eventual pedido de exclusão pelo Titular ou pela ANPD, sendo a conservação dos Dados Pessoais justificada por período superior no caso de cumprimento legal ou regulatório. Em outras palavras, salvo previsão legal, não será possível a guarda de Dados Pessoais por tempo indeterminado, motivo pelo qual é recomendável que sejam estabelecidos prazos de armazenamento para os Dados Pessoais submetidos ao Tratamento e que ocorra numa fiscalização recorrente do cumprimento dos referidos prazos estabelecidos.

Podemos citar como exemplos, o tempo de guarda mínimo dos registros de acesso conforme previsão do art. 15 do Marco Civil pelo prazo de 6 (seis) meses, o prazo prescricional de 3 (três) anos disposto no artigo 206, §3º, V do Código Civil para propor ação de reparação civil ou, ainda, o prazo de 5 (cinco) anos conforme artigo 27 do Código de Defesa do Consumidor.

Para fins de armazenamento, mesmo que cessado os demais Tratamentos, deve ser assegurada pelo Controlador a utilização dos mecanismos de segurança da informação necessários para afastar o acesso não autorizado, comunicação não autorizada, apagamento ilícito, dentre outros incidentes de segurança.

O armazenamento dos Dados Pessoais pode ser feito de modo físico (cartões, fichas, papéis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (em mídias como CD, DVD, Blu-Ray, HD externo, pendrive, cartão de memória SD), em servidor ou serviço contratado para estes fins, desde que esse terceiro assuma, no mínimo, as diretrizes mencionadas neste Guia.

Os meios físicos e digitais de armazenamento dos Dados Pessoais devem garantir a sua qualidade, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de Tratamento.

Por fim, para o controle do tempo de guarda dos Dados Pessoais, recomenda-se que cada Concessionária disponha de uma tabela de temporalidade de Dados Pessoais, a fim de possuir um controle desses prazos.

4.9. BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Cientes que a Governança da Informação deva contemplar aspectos técnicos de tecnologia da informação, de governança e promoção de cultura, para que seja eficiente em sua finalidade de garantir proteção adequada à informação (incluído dados pessoais), destaca-se a seguir boas práticas em SI em conformidade com esses pilares estratégicos:

Infraestrutura de TI

- Utilização de antivírus atualizado;
- Utilização de criptografia na transmissão e armazenamento de informações, quando necessário;
- Manter registro de trilhas de auditorias (logs) nos sistemas utilizados;
- Utilização de firewall, lógico ou físico, para filtrar os dados que transitam nos ambientes informáticos da concessionária;
- Realizar o backup periódico das informações armazenadas nos ambientes lógicos;
- Realizar a segmentação de rede;
- Realizar testes de intrusão (Pentest) e Scan de vulnerabilidades;
- Utilizar VPN, quando necessário;
- Manter os sistemas internos utilizados atualizados;
- Realizar teste de phishing;
- Utilizar serviços de armazenamento em nuvem;
- Gestão de acesso para os ambientes lógicos da Concessionária, de modo que os ambientes acessados sejam personalizados aos colaboradores.

No que tange ao armazenamento ou processamento de dados em nuvem, é necessário que os requisitos de confidencialidade, integridade e disponibilidade sejam mantidos. Por isso, que independentemente da nuvem contratada, se Privada, Pública, Comunitária ou Híbrida, bem como os modelos de serviços associados, por exemplo, Infraestrutura como um serviço (IaaS), e Software como serviço (SaaS), estejam em conformidade com as diretrizes estratégicas definidas na Política de Segurança da Informação.

Nesta perspectiva, convém que a concessionária mapeie os riscos relacionados à segurança da informação relativos aos serviços em nuvem, e os gerencie, de modo, que adote ações aptas a reduzir os riscos identificados.

Ato contínuo, os ambientes em nuvens contratados, devem refletir outros normativos que estão relacionados à Segurança da Informação, como classificação da informação e gestão de acesso, garantindo acesso a ambientes personalizados de acordo com a permissão concedida ao colaborador. Isto significa que, além da análise prévia à contratação, relativo a aspectos de segurança fornecidos por este ambiente lógico, deve haver intermediação contínua com o provedor de nuvem para que estes requisitos sejam cumpridos.

Com isso, é indispensável que haja transparência quanto às funcionalidades e formas pelas quais são realizados os tratamentos de dados pelo ambiente em nuvem, para que tais descrições incorporem o próprio Programa de Governança em Privacidade e Governança da Informação da Concessionária.

Vencidas estas considerações, convém que as concessionárias, sempre que possível, utilizem de técnicas de anonimização dos dados, quando tratarem dados pessoais, para retirar a capacidade de identificação dessa informação. Pois, a Lei Geral de Proteção de Dados pessoais, como seu próprio nome sugere, se refere a dados pessoais, que são informações que em conjunto ou isoladamente, são capazes de identificar ou tornar identificável uma pessoa física.

Portanto, se retirada a capacidade de identificação dessa informação, esta não será mais caracterizada como dado pessoal, e com isso, não será mais passível de aplicação da LGPD, já que foge ao seu escopo.

Entretanto, é imperioso frisar que a anonimização dos dados deve ser um processo irreversível, portanto deve haver formas de realizar sua anonimização definitiva, pois se houver possibilidade de reidentificação do titular, retornaria ao status de dado pessoal, e, assim, a LGPD seria aplicada.

Para tanto, recomenda-se que, para utilização da anonimização, sejam utilizados meios técnicos razoáveis e disponíveis no momento do tratamento, por meio do qual um dado perde a associação, direta ou indiretamente, com o titular (art. 5, XI). Nesta perspectiva, segue abaixo, exemplos de técnicas de anonimização:

- **Aleatorização:** Esta técnica altera a veracidade dos dados, visando eliminar sua ligação com o Titular de dados pessoais. Quanto mais

imprecisos forem, melhor sua desconexão com o dado pessoal. Essa técnica, sozinha, não irá reduzir a possibilidade de individualização de um registro, mas pode proteger contra-ataques maliciosos e riscos de inferência, podendo, ainda, ser combinada com técnicas de generalização ou outras técnicas para garantir a impossibilidade de identificação de um Titular de dados pessoais;

- **Supressão:** É a técnica mais básica e envolve a remoção de alguns dados de identificação do registro de dados para reduzir sua identificabilidade, por exemplo, remoção de um determinado campo de dados do conjunto de dados;

- **Generalização:** Envolve a transformação de valores específicos em uma faixa mais ampla de valores, por exemplo, transforma a idade específica de um indivíduo, como 18 anos, em uma faixa etária, como 18-24 anos. Ela não permite, no entanto, a anonimização de forma efetiva, devendo-se utilizar de outras técnicas para que a anonimização seja apropriada;

- **Adição de ruído:** Envolve alternar os valores de identificação exclusiva de um indivíduo em um conjunto de dados pelos valores de identificação exclusiva de outro indivíduo no conjunto de dados, por exemplo, alterar a data de nascimento real (17/06/1988) pela data de nascimento de outro indivíduo a partir desse conjunto de dados (22/04/1990). Na avaliação sobre eventual utilização da Adição de Ruído deve ser considerado o impacto na qualidade dos dados em relação ao resultado da estatística;

- **Permutação:** Essa técnica mistura, de forma aleatória, os valores de atributos existentes em tabela, fazendo com que estes dados sejam ligados artificialmente a Titulares de dados pessoais diferentes. É considerada uma forma especial de adição de ruído, que, assim como aquela, pode ser não oferecer sozinha as salvaguardas necessárias para que a anonimização seja adequada, devendo ser combinada com remoção de outros atributos identificadores.

Destaca-se que a técnica a ser utilizada deve ser referente à anonimização dos dados e não pseudonimização, já que este último processo permite a reidentificação dos dados a partir de informações adicionais, ou seja, os dados continuam com a possibilidade de identificar os titulares, e por isso não fogem da caracterização de dados pessoais.

Outro pilar essencial da Segurança da Informação é a Governança, que é concretizada pelas ações institucionais adotadas pelas Concessionárias com a finalidade de estabelecer procedimentos, através de normativos, que resguardam as informações. Exemplo de normativos que cumprem com essa finalidade são:

Governança

- **Política de Segurança da Informação:** com o objetivo de estabelecer responsabilidades, competências e diretrizes estratégicas para uso seguro dos ativos informáticos das concessionárias, e apoiar o Sistema de Gestão de Segurança da Informação;
- **Norma de Uso de Recursos de Tecnologia da Informação:** estabelecerá as restrições e regras específicas quanto ao uso dos Recursos de Tecnologia da Informação e Comunicação;
- **Norma de Classificação da Informação:** que definirá as regras para classificação e tratamento da informação de propriedade ou sob responsabilidade da concessionária;
- **Norma de Gestão de Acesso:** que definirá a forma pela qual a concessionária deve realizar a gestão de identidade e controle de acesso lógico aos seus ativos informáticos;
- **Norma de Gestão de Continuidade de Negócios:** estabelecerá rotinas e procedimentos para assegurar a não interrupção das atividades do negócio, proteger os processos críticos contra efeitos adversos ou desastres, considerando a sua retomada em tempo hábil e em consonância com as diretrizes de segurança da informação;
- **Norma de Gestão de Incidentes:** que irá dispor sobre controles de segurança necessários para assegurar que incidentes sejam tratados de forma efetiva, com ações corretivas para minimizar o impacto negativo sobre a Concessionária.

Quanto ao último pilar da Governança da Informação, a cultura não somente é igualmente importante como os outros pilares, como também os complementa. Pois de nada adiantaria ter normas quanto à segurança da informação se estas não estão sendo cumpridas pelos colaboradores da Concessionária, ou possuir a última tecnologia de segurança da informação se a vulnerabilidade do sistema de defesa for humana.

Nesta perspectiva, é necessário que as Concessionárias promovam treinamentos e elaborem materiais de conscientização para seu corpo colaborativo, sobre as práticas corporativas que resguardam a informação, com a finalidade de engajar toda a equipe.

Cultura

- Treinamentos sobre os normativos publicados, para que sejam de fato implementados;
- Treinamento sobre boas práticas em Segurança da Informação;
- Treinamento sobre gestão de crises e sala de crise quando da ocorrência de um incidente;
- Comunicados internos sobre riscos ao manusear informações, sobre engenharia social, sobre ameaças comuns (como ransomware e phishing), sobre condutas humanas (do and dont's);
- Gamificação de temas relacionados à Segurança da Informação e Proteção de Dados Pessoais;

Sobre a promoção da educação digital ou cultura, muitas podem ser as estratégias adotadas pelas concessionárias, de modo que não se limite somente aos exemplos supracitados, mas que seja adequado ao próprio contexto em que seu corpo colaborativo está inserido, e assim, desenvolva o planejamento educativo de maneira que incorpore as práticas recomendadas nas atividades diárias dos colaboradores.

4.10. DA INAPLICABILIDADE DA LGPD NAS EXCEÇÕES PREVISTAS NO ARTIGO 4º, INCISO III DA LGPD

Com relação às exceções de aplicação da LGPD ao Tratamento de Dados Pessoais previstas no artigo 4º, inciso III e nos §§ 1º e 2º, no caso de empresas privadas que tratem de Dados Pessoais para fins de prestação de serviço público, as Concessionárias não poderão se valer livremente dessas exceções, visto que a própria LGPD já prevê base legal para este tipo de operação.

Um exemplo disso é o disposto pelo art. 7 º, inciso III da LGPD, que prevê que o Tratamento de Dados Pessoais só será realizado pela Administração Pública com a finalidade de Tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Ademais, o próprio §1 º do art. 4º prevê que o Tratamento de Dados Pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observado o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD. Logo, quando falamos em concessões do poder público a entes privados para Tratamento de dados, o esperado é que a legislação aplicável ao caso esteja prevista no próprio edital de licitação.

Ainda no que diz respeito ao uso de legislação específica, podemos usar o exemplo de quando o Poder Público (por exemplo, a Polícia) solicita os dados de uma placa de veículo, aplicação à legislação pertinente do DETRAN, ou seja, uma lei geral que estabelece princípios gerais sobre o uso desses dados.

Por fim, ainda que exista uma base legal para o Tratamento de Dados Pessoais realizado pelas Concessionárias, recomenda-se que este compartilhamento feito com terceiros siga as diretrizes indicadas no item 5.3 deste Guia.

5. PROTOCOLOS

A seguir, apresentam-se alguns protocolos a serem seguidos pelas concessionárias com a finalidade de adequar suas atividades às regras e diretrizes apontadas pelas legislações e regulamentações de privacidade e proteção de dados pessoais aplicáveis:

5.1. PROTOCOLO DE PORTABILIDADE

O direito a portabilidade de dados pessoais está previsto no art. 18, inciso V da LGPD, o qual dispõe que:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...]
>
> V - **portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa**, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

A portabilidade verifica-se na possibilidade de copiar e transferir dados pessoais do titular, inseridos em um determinado serviço ou produto, viabilizando sua reutilização em outro serviço ou produto similar, assim como para outro possível uso.[11]

Referido direito não foi uma novidade trazida pela Lei Geral de Proteção de Dados (LGPD), eis que o regulamento europeu (GDPR) e algumas legislações norte americanas, como a legislação da Califórnia (California Consumer Privacy Act - CCPA), também já previam o direito a portabilidade de dados pessoais.

Como visto, o titular poderá requerer a portabilidade de seus dados aos controladores, os quais deverão transferir os dados pessoais para outros fornecedores. Ocorre que, a LGPD não tratou de diversos pontos que devem ser considerados quando da portabilidade, como por exemplo quais medidas de segurança devem ser adotadas, qual o limite considerando questões de segredo comercial e industrial, qual o meio e formato indicado para o atendimento à solicitação, como adotar padrões de interoperabilidade, entre outras situações.

11 In: Reflexões sobre proteção de dados pessoais em redes sociais. Revista Internacional de Protección de Datos Personales. Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia). Nº 1 Julio, Diciembre de 212. Disponível em https://habeasdatacolombia.uniandes.edu.co/wpcontent/uploads/10_Danilo-Doneda_FINAL

O que a legislação aponta é que a Autoridade Nacional de Proteção de Dados (ANPD) irá regulamentar sobre o tema. Entretanto, considerando que o tema ainda não foi regulamentado, apresentamos as boas práticas para o atendimento à portabilidade levando em conta aspectos de privacidade e segurança da informação.

PASSO A PASSO

Passo 1

Quando da solicitação de portabilidade pelo titular, considerando que os dados portáveis são aqueles referentes ao próprio titular, há **a necessidade de confirmação da identidade do solicitante**, assim como em qualquer outro atendimento à requisição de direito dos titulares;

Passo 2

Verificada a identidade do titular, passa-se à **análise de quais dados serão transmitidos a determinado fornecedor**. Cabe destacar aqui, que a LGPD dispõe que a portabilidade não inclui dados que já tenham sido anonimizados pelo controlador (art. 18, §6º da LGPD).

Passo 3

Por fim, recomenda-se que, quando da transmissão dos dados pessoais, que esta **seja realizada considerando questões de segurança da informação**, de forma a não comprometer a confidencialidade, disponibilidade e integridade dos dados pessoais.

!

ATENÇÃO:

Porquanto ausente de regulamentação, as Concessionárias não se consideram obrigadas a atender padrões específicos quanto ao formato ou outras especificidades a respeito da portabilidade, atentando-se assim tão somente às diretrizes ora postas na lei.

5.2. PROTOCOLO PARA O TRATAMENTO DE DADOS PESSOAIS EM ACIDENTES

O atendimento e monitoramento de acidentes que ocorrem nas vias de responsabilidades das Concessionárias são atividades recorrentes. Dessa forma, para que haja o correto tratamento dos dados pessoais, considerando as legislações e regulamentações, especialmente a LGPD, alguns pontos devem ser observados. Vejamos:

Desde o atendimento pré-hospitalar fornecido ao usuário até o registro e guarda das informações do acidente ocorrido, diversos dados pessoais são tratados e, muitos deles, por se tratar de dados de condições de saúde do titular, são considerados como dados pessoais sensíveis.

Entretanto, não é porque existem dados pessoais sensíveis que as Concessionárias não podem realizar o tratamento ou armazenar informações. O registro das informações dos acidentes, inclusive com fotos, é necessário para que em eventual ação judicial, a Concessionária consiga provar que não foi responsável pelo ocorrido, seja por falta de pavimentação, sinalização das vias, entre outros.

Dessa forma, apresenta-se algumas recomendações quanto ao tratamento dos dados pessoais nessas situações:

1. **Inserção das atividades de tratamento realizada no Registro das Operações de Tratamento (ROPA):** inicialmente, faz-se necessário que as atividades realizadas (seja para atendimento pré-hospitalar, registro do incidente, filmagens ou compartilhamento de informações) sejam registradas no ROPA, de forma que fique evidenciado todas as atividades de tratamento de dados pessoais, quais são os dados pessoais tratados e sua natureza (dados pessoais ou dados sensíveis), as categorias dos titulares (usuário, testemunha, colaborador, terceiro, entre outros) e as formas de armazenamento dos dados em questão.

2. **Identificação de uma base legal para os tratamentos realizados:** com base nas atividades realizadas e suas respectivas finalidades, as bases legais de tratamento devem ser identificadas para a legitimação do tratamento realizado. Por exemplo, o atendimento pré-hospitalar, caso realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, poderá ser legitimado na base legal de tutela da saúde. Igualmente, o registro do acidente, que contenha a descrição do ocorrido, fotos e demais informações dos titulares envolvidos, quando da finalidade de prevenção de ações judiciais de responsabilização, poderá ser baseado no exercício regular de direito. Para mais diretrizes quanto a aplicação de bases legais, vide item 3.4 do presente Guia.

3 **Avaliação da necessidade de elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** Considerando que no contexto de acidente há o tratamento de dados pessoais de saúde (dados pessoais sensíveis), a Concessionária deve considerar a elaboração de um RIPD, de forma a documentar a atividade de tratamento em questão, descrevendo os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, as medidas, salvaguardas e mecanismos de mitigação dos riscos identificados.

DÚVIDAS

E se a vítima do acidente (titular usuário) solicitar cópia dos registros?

Referida solicitação, trata-se do exercício do direito de acesso pelo titular. Assim, o fluxo para o atendimento de requisições dos titulares implementado internamente na Concessionária deve ser seguido. Para mais informações quanto ao atendimento dos direitos dos titulares, vide item 3.6 do presente Guia.

E caso terceiros, autoridade policial e demais entes solicitem os registros?

Quando da solicitação de acesso aos dados pessoais, por terceiros, autoridade policial e demais entes públicos, recomenda-se o seguimento do protocolo de compartilhamento de dados pessoais apresentado no item 5.3 do presente Guia, de forma que a solicitação seja analisada, conforme a finalidade, legitimidade, necessidade e demais requisitos legais e regulatórios aplicáveis ao caso em questão.

5.3. PROTOCOLO DE COMPARTILHAMENTO DE DADOS PESSOAIS

O compartilhamento de dados pessoais, nos termos da LGPD, verifica-se na comunicação, difusão, transferência nacional ou internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoais, e para uma ou mais modalidades de tratamento.

Nesse sentido, considerando as peculiaridades das Concessionárias, faz-se necessário identificar os principais cenários de compartilhamento, quais sejam:

1. o compartilhamento de dados pessoais em razão de obrigação legal ou regulatória, em que a Concessionária realiza o compartilhamento, mediante solicitação ou não do Ente Público;
2. o compartilhamento de dados pessoais com o poder concedente e/ou parceiros, decorrente da relação contratual firmada (execução do contrato);
3. o compartilhamento de dados pessoais em razão de uma solicitação pontual realizada por um Ente Público; e,
4. o compartilhamento com terceiros, mediante solicitações diversas.

No **primeiro cenário**, o compartilhamento é obrigatório e deve ser realizado considerando que, do contrário, a Concessionária estaria sujeita a incorrer em sanções por descumprimento legal. Referido compartilhamento, terá como fundamento os arts. 7º, inciso II e 11, inciso II, alínea a da LGPD: para o cumprimento de obrigação legal ou regulatória pelo controlador. Reforçando-se que mesmo o ente destinatário observará responsabilidades quanto ao tratamento dos dados recebidos, a partir deste momento, por fazê-lo para uma finalidade própria.

Veja alguns exemplos de fluxos relacionados ao compartilhamento de dados com entes públicos em decorrência de obrigação legal:

- Comunicação de acidente de trabalho do colaborador por determinação da Lei nº 8.213, de 24 de julho de 1991;
- Prestação de informações trimestrais e anuais à Agência Nacional de Transportes Terrestres – ANTT, nos termos da Resolução ANTT nº 2.495 de 13/12/2007.

Já, no **segundo cenário**, o compartilhamento de dados pessoais com o poder concedente e/ou parceiros, decorre da relação contratual firmada (execução do contrato). Veja alguns exemplos:

- Compartilhamento com o Poder Concedente do Diário operacional, com a finalidade de registrar acontecimentos diários que possam gerar risco à

operação ou integridade dos usuários ou colaboradores; e,

- Compartilhamento com Parceiros de comunicação de informações para aprovar conteúdo de publicidade.

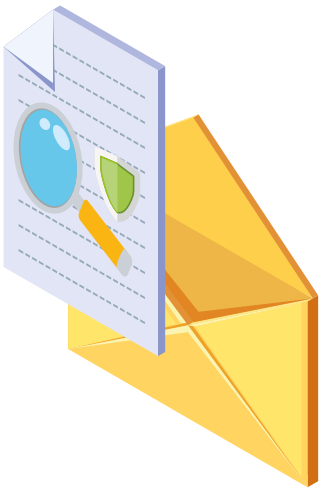
Nesses casos, ainda que o compartilhamento possa ser realizado com base no art. 7º, inciso V e art. 11, inciso II, alínea d da LGPD, ou seja, para execução do contrato ou procedimentos preliminares, faz-se necessário que a Concessionária avalie a finalidade do tratamento e a necessidade do compartilhamento dos dados pessoais em questão, para que sejam compartilhados apenas os dados estritamente necessários à finalidade contratual estabelecida.

No **terceiro cenário** o compartilhamento não é sempre necessário. Existem situações em que a Concessionária pode ser demandada por um Ente Público, solicitando informações que envolvam o compartilhamento de dados pessoais, no âmbito de um processo administrativo, por exemplo. Ou ainda, demandas pontuais que podem ter qualquer tipo de escopo. Nesses casos, recomenda-se que a Concessionária realize uma análise do pedido antes do compartilhamento dos dados pessoais.

Por fim, no **quarto cenário**, quando da solicitação de informações por terceiros que não possuem relação jurídica estabelecida com a Concessionária, igualmente deve ser realizada uma análise do pedido antes do compartilhamento dos dados pessoais.

Para a análise do pedido de compartilhamento nos cenários mencionados, faz-se necessário que a Concessionária observe os seguintes pontos:

1 Análise da Solicitação



Ao receber um pedido de compartilhamento de dados pessoais a concessionária deverá, antes do compartilhamento, analisar a solicitação considerando a natureza dos dados pessoais solicitados, a categoria de titular, o embasamento legal pela LGPD que legitime o compartilhamento, a necessidade, adequação e finalidade da solicitação.

Nos termos do art. 6º, inciso I da LGPD, cumprir com o princípio da a finalidade significa realizar o tratamento dos dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular.

Dessa forma, deve-se **analisar qual é a finalidade da solicitação feita, de forma a identificar o que o solicitante deseja realizar com esses dados pessoais**.

Trata-se de uma atividade legítima? Em conformidade com o ordenamento jurídico? É específica ou recai sob um tratamento genérico (sem finalidade determinada)?

Casos em que o solicitante não informe o motivo pelo qual necessita dos dados pessoais em questão, a não ser que já esteja previamente indicado em contrato firmado, recomenda-se que a Concessionária **questione qual é a finalidade**.

Não obstante, deve ser feito uma **análise quanto a compatibilidade das finalidades informadas com o contexto de tratamento**, considerando quais dados pessoais estão sendo solicitados e por qual motivo, de forma a cumprir com o princípio da Adequação.

Conforme o inciso II, do art. 6º da LGPD, a adequação consiste na compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Aqui, deve igualmente ser **analisada a necessidade de tratamento de todos os dados pessoais solicitados**, de forma que o compartilhamento trate o mínimo de dados pessoais necessários para atingir a finalidade informada pelo solicitante.

A LGPD conceitua o princípio da necessidade como a 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 (Art. 6º, III, da LGPD).

Dessa forma, a concessionária deve **ponderar se os dados pessoais solicitados cumprem com a finalidade indicada pelo solicitante**, bem como se o rol de dados pessoais solicitados é adequado e necessário à finalidade informada.

Caso contrário, a concessionária poderá requisitar informações complementares ao solicitante, bem como questionar o motivo de coleta dos dados pessoais considerados "excedentes".

Não obstante, quando do compartilhamento dos dados pessoais, deve-se igualmente **identificar em qual hipótese legal (Art. 7º e Art. 11 da LGPD) o tratamento será legitimado**. Para isso, a finalidade do tratamento deve ser levada em consideração para melhor adequação da base legal de tratamento.

Por fim, cabe destacar que o Poder Público apenas poderá tratar dados pessoais, 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, nos termos do art. 23 da LGPD.

Ainda, o mesmo artigo determina que o Poder Público, quando do tratamento de dados pessoais, informe as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, de modo que forneça 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.

Por conseguinte, em casos de solicitação em que a concessionária avaliou que o tratamento não possui uma finalidade determinada ou que os dados pessoais solicitados não são adequados e necessários ao objetivo do tratamento informado pelo Ente Público, recomenda-se que não seja realizado o compartilhamento antes de sanar tais questões.

2 Compartilhamento dos Dados Pessoais

Após a análise acerca dos requisitos de conformidade com a Lei Geral de Proteção de Dados (LGPD), a Concessionária deve avaliar acerca do compartilhamento ou não.

Quando a Concessionária entender que o compartilhamento não deve ser realizado, recomenda-se que forneça uma justificativa de recusa do compartilhamento ao solicitante.

Quando a Concessionária entender pelo compartilhamento, é importante que medidas de segurança sejam adotadas com a finalidade de prevenir acessos não autorizados às informações. Para isso recomenda-se:

- A inserção de senhas nos documentos a serem enviados, de forma que a senha seja compartilhada apenas com o destinatário em um e-mail em separado do arquivo encaminhado. Dessa forma, o risco de acesso não autorizado é reduzido; e,
- A utilização de link com acesso restrito apenas aos interessados, de forma a evitar a utilização apenas por e-mail.
- Um aviso a ser inserido no corpo do texto do e-mail, descrevendo que o documento contém dados pessoais, a finalidade do seu envio e a necessidade de ser tratado com sigilo.

O registro dos compartilhamentos de dados pessoais deve ser realizado pela Concessionária, para que esta possa fornecer as informações quando da solicitação pelo titular, conforme estabelece o art. 18, inciso VII quanto ao direito de obter informações do controlador (Concessionária).

É ainda necessário observar que, caso o titular solicite a correção, eliminação, anonimização ou bloqueio, a Concessionária informe aos agentes com os quais tenha realizado uso compartilhado de dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional (art. 18, §6º, LGPD).

Por fim, recomenda-se que a Concessionária garanta que que ao exportar dados pessoais de seus sistemas e importar aos sistemas dos Entes Públicos, Poder Concedente e/ou Parceiros, que os atributos da segurança da informação (CID: Confidencialidade, Integridade e Disponibilidade) não sejam violados.

Para melhor compreensão das medidas acima indicadas, apresenta-se exemplos práticos:

Compartilhamento de dados com terceiros:

Um usuário realizou uma solicitação de acesso a imagens da rodovia, com a finalidade de identificar a placa do carro e, consequentemente, o condutor que "supostamente" havia batido em seu carro. Nesse caso, a Concessionária deve conceder as informações ao solicitante?

Inicialmente, cumpre esclarecer que **a placa do veículo é considerada como dado pessoal**, pois ainda que não identifique diretamente o titular, este é passível de identificação. Dessa forma, referido compartilhamento deve observar as disposições trazidas pela LGPD.

Ainda, em relação **à imagem do titular**, que pode eventualmente aparecer nas gravações, esta também é **considerada como dado pessoal**, pois há a possibilidade de identificação do titular. Nota-se, aqui, que a imagem apenas será considerada como dado pessoal sensível, quando os meios do tratamento buscarem a identificação da pessoa através de tecnologias, por exemplo, por uso de reconhecimento facial. Do contrário, será considerada apenas como dado pessoal.

Esclarecidos esses pontos, a Concessionária deve avaliar o pedido de compartilhamento das informações considerando: (i) a finalidade do compartilhamento; (ii) a necessidade e adequação do tratamento dos dados pessoais em questão; (iii) a existência de uma base legal de tratamento que legitime o compartilhamento; e, (iv) quais medidas de se-

gurança devem ser adotadas, caso o compartilhamento seja realizado.

No caso em questão, o monitoramento da rodovia é uma atividade realizada pela Concessionária, por força de obrigações regulatórias e contratuais, ou seja, é uma atividade de tratamento de dados legítima. Entretanto, o compartilhamento de dados pessoais como placa de veículo e imagens a terceiros não se verifica em uma prática segura, eis que não há como comprovar que o requisitante possui legitimidade para acesso a esses dados pessoais. Dessa forma, a Concessionária deve fornecer instruções ao requisitante no sentido de realizar um pedido de acesso às imagens judicialmente ou através de uma autoridade policial. Isso porque, para o cumprimento de determinação legal/judicial, existe base legal (art.7º) aplicável ao caso.

Compartilhamento de dados com o DETRAN:

O DETRAN solicitou o acesso a imagens da rodovia para emissão de notificação de trânsito. Nesse caso, como a Concessionária (Federal) deve proceder?

Considerando que o DETRAN é um órgão fiscalizador, o pedido deve ser analisado de forma a identificar: (i) a finalidade do compartilhamento; (ii) a necessidade e adequação do tratamento dos dados pessoais em questão; (iii) a existência de uma base legal de tratamento que legitime o compartilhamento; e, (iv) quais medidas de segurança devem ser adotadas, caso o compartilhamento seja realizado.

Pois bem, nos termos do art. 2º da Resolução nº 2.064/2007 da ANTT, que dispõe sobre a utilização de sistema de monitoramento de tráfego por meio de Circuito Fechado de Televisão - CFTV em concessões rodoviárias federais reguladas pela ANTT, "Art. 2º **O monitoramento do tráfego, via sistema de CFTV, deve possibilitar** o acompanhamento das condições de fluidez na rodovia e dinamizar os serviços de socorro médico e mecânico, a se-

gurança viária e **a disponibilização de informações aos usuários e órgãos de trânsito**".

Ainda, o artigo 11 dispõe que "**É facultado à concessionária estabelecer convênio com os órgãos fiscalizadores de trânsito para cessão de link, possibilitando o acesso remoto às imagens captadas em tempo real**."

Nesse sentido, verifica-se que a **finalidade da solicitação é legítima** e que a Concessionária poderá **legitimar o compartilhamento das imagens da rodovia no inciso V do art. 7º da LGPD**, ou seja, para cumprimento do contrato de convênio.

As medidas indicadas nesse protocolo devem ser adotadas para que o compartilhamento de dados pessoais seja realizado em conformidade com as legislações e regulamentações de privacidade e proteção de dados pessoais aplicáveis.

!

ATENÇÃO:

Acidentes podem envolver a necessidade de compartilhamento de dados de cunho médico e de saúde, e que, inclusive, podem estar ligados à noção de sigilo médico. Para tanto, quando do compartilhamento desses dados com pessoas não habilitadas diretamente e que se apresentem na qualidade de representantes do Titular, deve-se atentar à comprovação de que o mesmo Titular não o possa solicitar por si; que este consiga confirmar aquele como seu representante; ou na impossibilidade total, que, através dos requisitos acima descritos no protocolo, se observem os princípios, as hipóteses legais, e eventualmente direcionem o solicitante ao poder público para validar sua solicitação, sendo mesmo o caso, se necessário, de que as Concessionárias o façam como meio de resguardar-se aos seus direitos.

5.4. SITUAÇÕES ADICIONAIS

BASE LEGADA

Como anteriormente indicado, a base legada é uma base de dados pessoais para os fins da LGPD, assim, os dados nela contidos devem seguir as mesmos diretrizes da lei para os demais dados pessoais, com a ressalva de que o tema ainda precisa ser regulamentado pela ANPD.

Se não houver condições de fato para sanitizar a base, ou aplicar as diretrizes da lei para o tratamento de dados pessoais realizados para a base legada, há justificativa válida para impedir o acesso aos dados que não estejam sendo tratados porquanto não há regulamentação. Reiterando-se que a mera inexistência de regulamentação, a depender do perfil dos dados tratados, pode mesmo assim representar riscos evidentes ao Titular de dados pessoais, razão pela qual cada hipótese deve ser analisada com profundidade.

SOLICITAÇÃO DE ACESSO COM APRESENTAÇÃO DE DOCUMENTO DESATUALIZADO

Nestes casos a análise será sempre pautada pela finalidade e necessidade atreladas ao tratamento, dependendo sempre do tipo de informação solicitada e dos dados atrelados a esta. Se os dados pessoais requeridos são dados comuns, como aqueles de acesso, identificação simples etc., a mera comprovação da identidade não pode forçar o requerente que o faça por um documento atualizado para o ano do pedido, posto que tais documentos são sempre atualizados com grande lapso de tempo (lembrando que a apresentação de um documento de identidade que não permita o reconhecimento da pessoa que o apresenta, como nos casos em que o documento contém foto da pessoa ainda na infância, valida a exigência de apresentação de documento com foto atual, ou seja, que permita identificar o apresentante como tal). Nas hipóteses em que se constatar que os dados pessoais solicitados podem representar riscos a terceiros e não mais pertencer a um determinado Titular, por condição temporal, a comprovação de período atualizado se torna necessária, assim, nesses casos, é válida a solicitação de comprovação que garanta que o pedido é válido para aquele período.

DOCUMENTOS VÁLIDOS PARA COMPROVAÇÃO DA IDENTIDADE DO REQUERENTE

Em suma, não se trata do documento apresentado, mas da hipótese em si. A mera apresentação do documento de identidade do requerente pode servir como meio comum de comprovação (envio de cópia simples, por exemplo), sendo igualmente válida a solicitação de informações adicionais que permitam confirmar a identidade (como validar o endereço ou telefone cadastrado, se houver cadastro anterior). A solicitação por formulário pode ser aplicada, bem como, se a hipótese envolver risco complexo, o reconhecimento de firma ou autenticação do documento apresentado.

REQUERIMENTO DE ACESSO A DADOS PESSOAIS EM CONCESSÃO COM ATIVIDADES ENCERRADAS

Nas hipóteses em que se verificar qualquer das disposições do Art. 15 da LGPD, com as ressalvas do Art. 16, opera-se a negativa para o acesso aos dados que não mais estejam sob a guarda da Concessionária. Se por qualquer motivo houve a manutenção da base de dados, inclusive ocasional pela condição de atividade pública que abrange a concessão de rodovias, a relação com o Titular se mantém e este pode ter acesso aos seus dados pessoais nos termos lei. Toda e qualquer necessidade de manutenção deve ser avaliada com o apoio dos envolvidos com os temas de proteção de dados pessoais de cada empresa.

SOLICITAÇÃO DE DADOS DE VEÍCULOS ATRELADOS A EMPRESAS

Primeira questão envolve comprovar que o representante de fato o é, e mesmo aqui o tratamento de dados pessoais abrange apenas os dados que ingressas, ou seja, da pessoa que representa a organização. Quanto aos dados em si, se os veículos estão registrados em nome de uma empresa, não teremos aqui dados pessoais para além dos dados eventuais de seus representantes legais, mas tão somente dados comuns, informações sem vínculo à uma pessoa natural, logo, sem aplicação da LGPD. Se a solicitação envolver qualquer dado pessoal, mesmo que indireto, deve-se confirmar o Titular ou sua representação, e, se impossibilitada a veiculação imediata, indica-se que o requerente seja direcionado a acionar as autoridades competentes.

MELHORES RODOVIAS DO BRASIL

ABCR

abcr.org.br

/melhoresrodovias/

@melhoresrodovias

/MelhoresRodovias

/abcr_rodovias

@melhoresrodovias