Guia de Boas Práticas de Proteção de Dados no Setor de Transporte

CNT | SEST SENAT | ITL

LGPD
TRANSPARÊNCIA E SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

Expediente

CNT – SEST SENAT – ITL
Presidente do Sistema CNT
Vander Costa

MODAIS

Transporte Rodoviário de Passageiros
Vice-Presidente da CNT: Eudo Laranjeiras Costa
Presidente da Seção: Rubens Lessa Carvalho

Transporte Rodoviário de Cargas
Vice-Presidente da CNT: Flávio Benatti
Presidente da Seção: Eduardo Ferreira Rebuzzi

Transporte Aquaviário de Cargas e Passageiros
Vice-Presidente da CNT: Raimundo Holanda Cavalcante Filho
Presidente da Seção: Waldemar Rocha Júnior

Transporte Ferroviário de Cargas e de Passageiros
Vice-Presidente da CNT: Joubert Fortes Flores
Filho Presidente da Seção: Benony Schmitz Filho

Transporte Aéreo de Cargas e de Passageiros
Vice-Presidente da CNT: Eduardo Sanovicz
Presidente da Seção: Airton Nogueira Pereira Junior

Infraestrutura de Transporte e Logística
Vice-Presidente da CNT: Paulo Gaba Junior
Presidente da Seção: Murillo Moraes Rego Corrêa Barbosa

CNT - SEST SENAT - ITL

Diretor Institucional da CNT
Valter Souza

Diretor-Executivo da CNT
Bruno Batista

Diretora-Executiva Nacional do SEST SENAT
Nicole Goulart

Diretor-Executivo do ITL
João Victor Mendes

GRUPO DE TRABALHO PARA ELABORAÇÃO DO GUIA DE BOAS PRÁTICAS

Transporte Rodoviário de Passageiros
Matteus de Paula Freitas
Fernando Variani

Transporte Rodoviário de Cargas
Ana Carolina Ferreira Jarrouge
Narciso Figueirôa Junior

Transporte Aquaviário de Cargas e Passageiros
André Luiz Zanin de Oliveira
Fabio Castro

Transporte Ferroviário de Cargas e de Passageiros
Roberta Marchesi
Camila Costa

Transporte Aéreo de Cargas e de Passageiros
Antônio Augusto do Poço Pereira
Lívia Pinheiro Ferreira Nagato
Rafael Esnarriaga
Milena Itri Amadeo

Infraestrutura de Transporte e Logística
Paulo Miguel Jr.
Luciana Cardoso Guerise
Carla Pecora Gomes

Coordenação e elaboração
Danilo Doneda
Giovanna Milanez
Gabriel Souto
Daniele Doneda (design e diagramação)

Comitê de Governança de Dados do Sistema CNT
Dim Michelle Ferreira Rodrigues
João Frederico Chagas Maranhão
João Guilherme Abrahão
Luciana Malamin Correia

Sumário

Sumário

Apresentação

GUIA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS NO SETOR DE TRANSPORTE

Com o advento da LGPD (Lei Geral de Proteção de Dados Pessoais), a transparência, como um princípio básico, tornou-se ainda mais premente para as empresas que lidam com os dados pessoais dos seus clientes, fornecedores e colaboradores. Nesta nova era, o que parecia ser trivial deve ser encarado com cuidado redobrado pelo setor transportador. Afinal, a percepção dos dados pessoais como um ativo de valor intangível ganhou dimensão e forma.

Por esse motivo, o Guia de Boas Práticas de Proteção de Dados no Setor de Transporte é mais uma entrega do Programa Nacional LGPD no Transporte. O Sistema CNT vem envidando um conjunto de iniciativas para apoiar os transportadores no desenvolvimento de medidas para a proteção de dados pessoais, esclarecer os principais aspectos teóricos e práticos da LGPD e suas aplicações nos diferentes modos de transporte.

Esse trabalho está ancorado em três linhas: sensibilização, capacitação profissional e aplicação. Isso inclui a realização de eventos, o desenvolvimento de material informativo e a oferta de cursos de capacitação. Nesse sentido, esta publicação é mais uma aposta no sentido de sensibilizar os empresários e estabelecer padrões e protocolos para a fiel aplicação da LGPD nas empresas do transporte rodoviário, aquaviário, ferroviário e aéreo – sejam elas de cargas ou de passageiros –, e também as de infraestrutura de transporte e logística.

Outra demonstração na prática do que o Sistema CNT vem promovendo nessa seara são os cursos ofertados sobre o tema. Já capacitamos mais de 200 gestores de empresas com a primeira turma do curso executivo LGPD para o Setor de Transporte, promovido pelo SEST SENAT e coordenado pelo ITL, que ensina como

Apresentação

implementar a nova legislação. Já o curso LGPD Descomplicada, oferecido pelo SEST SENAT, qualificou aproximadamente 6.000 pessoas, entre trabalhadores do setor e comunidade.

Precisamos ter cada vez mais em mente que, com a LGPD, o Brasil ganha ainda mais respaldo no debate internacional sobre esse tema tão caro para a sociedade. E não temos de dúvidas de que essa é uma grande oportunidade para as transportadoras potencializarem os processos de modernização das suas gestões. Por isso, o Sistema CNT reafirma sua posição de, juntamente aos transportadores, sempre buscar o desenvolvimento pleno do setor e também contribuir para aprimorar o necessário ambiente de negócios no Brasil.

Vander Costa
Presidente do Sistema CNT

>> CAPÍTULO 1

Considerações Iniciais

1.1. INTRODUÇÃO

Este Guia de Boas Práticas de Proteção de Dados no Setor de Transporte tem o objetivo de estabelecer padrões e protocolos para o tratamento de dados pessoais, facilitando e otimizando a fiel aplicação da normativa de proteção de dados estabelecida pela Lei Geral de Proteção de Dados (Lei 13.709/2018) e demais normativas relacionada pelas empresas do setor de transporte, bem como colaborar com a Agência Nacional de Proteção de Dados (ANPD) e outros entes da administração pública na aplicação da LGPD no setor em suas diretrizes e parâmetros. O Guia foi elaborado por especialistas da área de proteção de dados em diálogo com membros da CNT/SESTSENAT/ITL e representantes dos diversos modais do setor.

Este Guia contém orientações gerais e específicas para os diversos modais de transporte: rodoviário, aquaviário, portuário, ferroviário e aéreo de passageiros e de cargas, bem como à infraestrutura de transporte e logística, em relação à implementação e adaptação das suas atividades à LGPD. Nele, estão contempladas as normativas já existentes na prestação de serviços de transporte de passageiros e de cargas, bem como serviços de logística e infraestrutura, à luz das normas de proteção de dados pessoais, nos termos vislumbrados pelo art. 50 da LGPD.

O setor de transporte engloba diferentes modais e, assim, diferentes modalidades de transporte, portanto é fundamental que se estabeleçam diretrizes gerais, aplicáveis a todo setor e adaptadas à realidade dos prestadores de serviço nele atuantes, a fim de garantir a aplicação e a efetividade da LGPD de forma mais concreta e específica. Este Guia de Boas Práticas pretende, diante da variedade de empresas e da própria peculiaridade do setor de transporte, traçar diretrizes gerais para o tratamento de dados pessoais a fim de garantir a observância efetiva da LGPD no setor.

No setor de transporte, além da observância das regras impostas pela LGPD, há que se considerar também a regulação e também a dinâmica própria do segmento. Para tal, este Guia contará com este capítulo de considerações iniciais, que explora os principais conceitos da LGPD, o âmbito de aplicação e a própria justificativa deste guia

para, a seguir, apresentar elementos e diretrizes referentes à aplicação da normativa de proteção de dados em situações determinadas e relevantes para o setor de transporte. Estas serão abordadas em protocolos gerais, aplicáveis a todo o setor de transporte, e também em protocolos especiais para determinadas situações que, ainda que não sejam de aplicação transversal para todo o setor, em virtude da sua complexidade ou da própria sensibilidade da atividade de tratamento, merecem atenção.

1.2. A LEI GERAL DE PROTEÇÃO DE DADOS: ARQUITETURA, FUNDAMENTOS E DEFINIÇÕES

Em vigor desde setembro de 2020, a Lei Geral de Proteção de Dados objetiva fornecer instrumentos e garantias para que os cidadãos possam exercer efetivamente o controle sobre os seus próprios dados pessoais, na linha dos mais de 140 países que já contavam com legislações semelhantes. Assim, a Lei nº. 13.709/2018 (LGPD) estabelece regras para o tratamento de dados pessoais[1] de forma ampla e geral, por pessoa natural ou jurídica, de direito público ou privado, em praticamente todos os setores e circunstâncias[2] - com um modelo horizontal e geral, a LGPD aplica-se a todos os setores econômicos da sociedade, incluindo o setor de transporte.

O elemento nuclear da inovação trazida pela LGPD ao ordenamento jurídico brasileiro é a noção de que não existem mais dados pessoais irrelevantes na atual sociedade da informação e, portanto, todo tratamento de dados pessoais deve ser ponderado a partir da sua legalidade e legitimidade em função da lei aplicável, visto ainda que os dados pessoais são projeção da personalidade e como tal devem ser considerados. Assim, estabelecido que qualquer tratamento de dados pessoais pode

1. O tratamento envolve qualquer operação realizada com os dados pessoais, incluindo a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais.

2. As exceções à aplicabilidade da LGPD (discriminadas no art. 4º da LGPD) são pontuais e referem-se quase sempre a situações nas quais há preponderância de interesse público específico. Ainda assim, o referido artigo assinala a necessidade de legislação específica determinar, na forma cabível, a proteção de dados na maior parte das situações excluídas nas quais a LGPD não se aplica.

gerar efeitos para o cidadão titular de dados, inclusive com o potencial de violar os seus direitos fundamentais, verifica-se necessária a consideração desses efeitos e a introdução de instrumentos que visem proporcionar tanto a proteção do cidadão como garantir a segurança no tratamento e no fluxo de dados pessoais, tema de relevância cada vez mais concreta para diversas atividades.

Assim, além de estabelecer critérios rígidos para o tratamento de dados pessoais, de forma a proteger a privacidade, a autodeterminação informativa, a intimidade, a honra, a imagem e a dignidade do titular dos dados, a LGPD considera igualmente a importância central dos dados pessoais para diversas dinâmicas da Sociedade da Informação e, portanto, preocupa-se igualmente em não deixar de lado o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência, procurando estabelecer um espaço de legitimidade para o tratamento de dados pessoais. Esse é o motivo pelo qual, inclusive, essas questões são diretamente mencionadas como fundamentos da disciplina da proteção de dados no art. 2º da Lei.

1.2.1. PRINCÍPIOS

A LGPD estabelece uma arquitetura para a tutela dos dados pessoais baseada em três pilares: (i) a verificação de legitimidade do tratamento de dados pessoais a partir da necessária vinculação de cada tratamento de dados a uma das bases legais elencadas nos seus artigos 7º e 11 e da sua compatibilidade com os princípios de proteção de dados; (ii) avaliação da obediência aos procedimentos que devem ser observados no tratamento de dados pessoais (a verificação dos princípios de proteção de dados e dos direitos do titular, bem como o cumprimento das obrigações dos agentes de tratamento) e (iii) o estabelecimento de meios para orientar, fiscalizar e, quando necessário, estabelecer sanções ou indenização para o caso de não cumprimento da Lei.

Os princípios de proteção de dados, dispostos no artigo 6º da LGPD, são uma espécie de núcleo duro da regulação dessa matéria. Estão previstos 11 (onze) princípios gerais norteadores para todo e qualquer tratamento de dados. Nessa

Considerações Iniciais

lógica, o tratamento de dados somente será legítimo caso (i) fundamente-se em uma base legal, que abordaremos a seguir, e (ii) observe os princípios da LGPD. O quadro abaixo explica de forma mais detalhada o escopo de cada um dos princípios previstos no art. 6º da Lei.

PRINCÍPIO DA BOA-FÉ OBJETIVA	O princípio da boa-fé, previsto no *caput* do art. 6º da LGPD, representa a imposição de uma regra de conduta (boa-fé objetiva), ou seja, um padrão de comportamento leal, baseado em uma conduta proba e transparente, que se materializa a partir da observância dos interesses legítimos e das expectativas razoáveis do titular, a partir de um tratamento que não lhe cause qualquer tipo de abuso, lesão ou desvantagem.
PRINCÍPIO DA FINALIDADE	O princípio da finalidade, previsto no art. 6º, I, da LGPD, exige que o tratamento de dados pessoais seja realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. Não há, portanto, tratamento de dados pessoais legítimo sem a consideração da sua finalidade.
PRINCÍPIO DA ADEQUAÇÃO	O princípio da adequação, definido no art. 6º, II, da LGPD, determina que deve haver compatibilidade entre o tratamento e as finalidades informadas ao titular, de acordo com o contexto do tratamento.
PRINCÍPIO DA NECESSIDADE	O princípio da necessidade, previsto no art. 6º, III, da LGPD, dispõe que o tratamento deve ser limitado 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. Este princípio da necessidade remonta à ideia da minimização do uso de dados pessoais, isto é, implica que a estes se deva reduzir ao mínimo possível a utilização de dados pessoais, dado o risco inerente que sua utilização apresenta.

Considerações Iniciais

PRINCÍPIO DO LIVRE ACESSO	O princípio do livre acesso, disciplinado no art. 6º, IV, da LGPD, exige que os agentes de tratamento garantam, aos titulares, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. O art. 9º da LGPD, inclusive, reforça tal princípio, determinando que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva quanto a, entre outras características: (i) a finalidade específica do tratamento; (ii) a forma e a duração do tratamento, observados os segredos comercial e industrial; (iii) a identificação do controlador; (iv) as informações de contato do controlador; (v) as informações sobre o uso compartilhado de dados pelo controlador e a finalidade; (vi) as responsabilidades dos agentes que realizarão o tratamento; e (vii) os direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.
PRINCÍPIO DA QUALIDADE DOS DADOS	O princípio da qualidade dos dados, previsto no art. 6º, V, da LGPD, exige que os agentes de tratamento garantam, aos titulares, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
PRINCÍPIO DA TRANSPARÊNCIA	O princípio da transparência, disposto no art. 6º, VI, da LGPD, exige que os agentes de tratamento garantam, aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
PRINCÍPIO DA SEGURANÇA	O princípio da segurança, previsto no art. 6º, VII, da LGPD, determina que sejam utilizadas, no tratamento, 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.

Considerações Iniciais

PRINCÍPIO DA PREVENÇÃO	**O princípio da prevenção, disciplinado no art. 6º, VIII, da LGPD, impõe que sejam adotadas previamente medidas para diminuir riscos e possíveis danos aos titulares nos tratamento de dados pessoais.**
PRINCÍPIO DA NÃO DISCRIMINAÇÃO	**O princípio da não discriminação, disposto no art. 6º, IX, da LGPD, proíbe a realização do tratamento para fins discriminatórios ilícitos ou abusivos.**
PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	**O princípio da responsabilização e prestação de contas, previsto no art. 6º, X, da LGPD, exige que os agentes de tratamento demonstrem a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.**

Os princípios de proteção de dados previstos na LGPD fornecem diretrizes gerais de conformidade do tratamento. Ou seja, sempre que for necessário analisar se determinado tratamento de dados pessoais é efetivamente lícito será necessário avaliar o cumprimento dessas diretrizes gerais. Para que isso fique ainda mais claro, destaca-se o exemplo abaixo, que ilustra como uma avaliação de compatibilidade deve ser realizada à luz do princípio da finalidade[1].

1. O exemplo foi extraído do Parecer 3/2013 sobre limitação da finalidade, adotado em 2 de abril de 2013 pelo Grupo de Trabalho de Proteção de Dados do Artigo 29.

Considerações Iniciais

>> EXEMPLO 1

UTILIZAÇÃO DE TESTES COM ETILÔMETRO PARA CONTROLE DA PONTUALIDADE DE MOTORISTAS

Uma empresa de transporte público ou de carga exige que os motoristas de ônibus, todos os dias antes de iniciar seu turno, soprem em um etilômetro (também conhecido como bafômetro) para verificar a presença de álcool. A hora e a data do teste são registradas, juntamente com as informações sobre o resultado do teste. Este procedimento está integrado a um sistema de entrada e saída no trabalho, ou seja, quando os motoristas de ônibus começam seu turno, eles são obrigados a autenticar o seu cartão de identificação e a soprar no etilômetro.

O objetivo da coleta e tratamento desses dados, conforme previsto na legislação e também comunicado aos funcionários, é verificar se os motoristas possuem quantidade não autorizada de álcool no corpo durante o turno de trabalho, o que infringiria a lei.

No entanto, na eventualidade que este procedimento também seja, sem o conhecimento dos motoristas, utilizado para verificar se os motoristas cumpriram suas obrigações em termos de jornada de trabalho, ou seja, se eles chegaram pontualmente no início de seu turno, ou se os resultados sejam eventualmente armazenados e utilizados para quaisquer outras finalidades que não estejam abarcadas pela legislação, surgem questionamentos relevantes ligados à legitimidade deste tratamento de dados.

Além das preocupações de natureza trabalhista que este exemplo possa levantar, pode-se dizer que um titular de dados presumiria razoavelmente que os etilômetros são utilizados para verificar unicamente a presença de álcool, mas não para outros propósito não relacionados.

Isso já é um forte indicativo de que o uso posterior desses dados para outras finalidades, como o controle de jornada ou outras, pode ser incompatível. Há fatores importantes que devem ser levados em consideração, como o potencial impacto negativo sobre o funcionário (por exemplo, a aplicação de uma possível sanção disciplinar), a natureza sensível dos dados registrados pelo etilômetro, a obrigação legal do funcionário em fornecê-los, o desequilíbrio de poder entre o titular dos dados e o empregador e a falta de salvaguardas adicionais (como, por exemplo, a notificação sobre outras finalidades além da verificação dos limites de álcool) podem contribuir e confirmar esta avaliação.

O mesmo exemplo se aplica aos motoristas de caminhão ou veículos de pequeno porte para o transporte de cargas, quando as empresas realizam o teste com etilômetro para identificar a presença de álcool antes do motorista iniciar a viagem ou as entregas/coletas. A expectativa do motorista é que o controle seja em razão da segurança de trânsito e cumprimento da legislação vigente, e não para controle de pontualidade com relação ao cumprimento de jornada, o que configuraria um desvio de finalidade.

1.2.2. CONCEITOS

A LGPD, ao atribuir relevo jurídico aos dados pessoais e às operações de tratamento com eles realizadas, trouxe consigo uma série de novos conceitos para o ordenamento jurídico brasileiro, seja para melhor delimitar seus institutos e sua aplicação, seja para melhor comunicar diversas de suas características que, em diversos aspectos, são inovadoras. Portanto, para compreender o verdadeiro escopo das operações de tratamento de dados e da aplicação da LGPD, é fundamental a plena familiaridade com os seus conceitos, iniciando com o próprio conceito de dado pessoal, que é, no final das contas, o elemento nuclear da Lei.

Para a LGPD, dado pessoal é toda e qualquer informação que identifique ou seja capaz de identificar um indivíduo, independente da sua natureza ou de seus atributos. Assim, os elementos cumulativos do conceito de dado pessoal são: (i) ser uma informação, de qualquer natureza, (ii) que esteja relacionada a uma pessoa natural (o titular dos dados), (iii) que identifique ou pelo menos tenha o potencial de identificar o seu titular.

Os dados que não se referirem a uma pessoa identificada ou identificável, portanto, não são dados pessoais e o seu tratamento não está sujeito às regras da LGPD. Da mesma forma, os dados anonimizados, que são basicamente dados pessoais que foram submetidos a um processo de anonimização, de forma a não identificar mais seus titulares, não são dados pessoais. Já em relação aos dados pseudonimizados, que podem ser reconduzidos aos seus titulares através de uma chave de identificação armazenada separadamente dos dados em si, estes continuam sendo caracterizados como dados pessoais e sujeitos à LGPD, ainda que seu tratamento apresente potencial de maior segurança aos titulares.

A LGPD não estabelece categorias ou subgrupos de dados pessoais, visto que parte do pressuposto de que todo dado pessoal merece proteção. No entanto, ela criou uma única tipologia especial para aqueles dados pessoais que, em virtude do seu conteúdo, podem colocar o seu titular em condição de vulnerabilidade específica, como no caso dos dados pessoais sensíveis. Aqui a preocupação é justamente proteger o titular de eventual discriminação em virtude de aspectos específicos da sua personalidade. Dessa forma, é possível categorizar os dados pessoais e seus agentes, à luz do regramento da LGPD, conforme o quadro abaixo.

Considerações Iniciais

CATEGORIA	DISPOSITIVO	CARACTERÍSTICA PRINCIPAL
DADOS PESSOAIS	Art. 5º, I	Informação relacionada à pessoa natural identificada ou identificável. Por exemplo, o nome, endereço, telefone, e-mail, conta corrente, nome dos filhos, data de nascimento, RG, CPF, além de qualquer outra informação que possa ser relacionada a uma pessoa.
DADOS PESSOAIS SENSÍVEIS	Art. 5º, II	Dados que proporcionam maior potencial discriminatório ao seu titular e que merecem proteção específica. São os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.
DADOS PESSOAIS PSEUDONIMIZADOS	Art. 13, § 4º	São dados pessoais cujo elemento identificador, capaz de remeter o dado ao seu titular, foi retirado e armazenado à parte para que os dados pseudonimizados possam ser tratados sem que os titulares sejam identificados. Sempre é possível identificar o titular de um dado pseudonimizado, porém somente a partir do uso de informação adicional, mantida separadamente. O procedimento de pseudonimização é utilizado para garantir maior segurança e diminuir o risco em tratamentos de dados pessoais. Em virtude da possibilidade de reidentificação do titular dos dados nesse caso, os dados pseudonimizados são considerados dados pessoais e encontram-se dentro do escopo de proteção da LGPD.

Considerações Iniciais

DADOS ANÔNIMOS OU ANONIMIZADOS	Art. 5º, III	Os dados anonimizados não permitem a identificação de seus titulares, pois foi aplicado um procedimento de anonimização pelo qual ele perde o seu elemento identificativo de forma a não poder ser recuperado, considerando os meios técnicos razoáveis e disponíveis no momento do seu tratamento. Os dados anonimizados estão fora do escopo da LGPD e, embora em sua origem fossem dados pessoais, deixam de ser cobertos pela LGPD dada a impossibilidade de serem relacionados aos seus titulares.
TITULAR	Art. 5º, V	É a pessoa natural (pessoa física) a quem se referem os dados pessoais que são objeto de tratamento. Pessoas jurídicas não são titulares de dados perante a LGPD.
CONTROLADOR	Art. 5º, VI	É a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais e a definição da sua finalidade. O controlador, assim, é quem possui poder de decisão sobre as finalidades e os elementos essenciais do tratamento de dados.
OPERADOR	Art. 5º, VII	É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador é um terceiro em relação ao controlador que atua de acordo com os interesses deste, sendo-lhe facultada apenas a definição de elementos não essenciais à finalidade do tratamento de dados. Faltando-lhe, portanto, o poder de decisão, o operador só pode agir no limite das finalidades determinadas pelo controlador.

Considerações Iniciais

AGENTES DE TRATAMENTO	Art. 5º, IX	Tanto o controlador como o operador são agentes de tratamento. São estes que realizam operações de tratamento de dados pessoais.
SUBOPERADOR	Sem previsão legal direta*	É aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador. A relação direta do suboperador é com o operador e não com o controlador. No que se refere à sua responsabilidade, o suboperador equipara-se ao operador perante a LGPD em relação às atividades que executa.
CONTROLADORIA CONJUNTA	Sem previsão legal direta; previsão incidental no art. 42, § 1º, II.	É o desempenho conjunto entre dois ou mais controladores das tarefas de determinar as finalidades e dos meios desse tratamento. No que se refere à responsabilidade, há consequências no que diz respeito às funções dos agentes de tratamento e aos direitos dos titulares, podendo responder de forma solidária.

** Ainda que não haja menção ao suboperador na LGPD, o conceito foi apresentado e explorado no "Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado", publicado pela Autoridade Nacional de Proteção de Dados[1].*

1. Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf

Considerações Iniciais

ENCARREGADO	Art. 5º, VIII	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). Deve-se assumir, como regra geral, que toda organização deverá indicar uma pessoa para assumir esse papel, cabendo eventualmente à ANPD estabelecer exceções em casos que não seja necessária a sua indicação.
TRATAMENTO	Art. 5º, X	Tratamento é qualquer operação que possa ser realizada com os dados pessoais, incluindo a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O conceito de tratamento é abrangente e envolve quaisquer atividades realizadas com o dado pessoal, sendo a relação de operações meramente exemplificativa.

Considerações Iniciais

1.2.3. BASES LEGAIS PARA O TRATAMENTO DE DADOS

A LGPD, ao reconhecer a importância e relevância jurídica dos dados pessoais, estabelece um conjunto restrito de hipóteses nas quais pode ser realizado o seu tratamento, que são as chamadas bases legais.

Há bases legais que são aplicáveis para o tratamento de dados pessoais em sua generalidade, previstas no art. 7º da LGPD. Há, especificamente, um conjunto reduzido de bases legais aplicadas para o tratamento de dados pessoais sensíveis, previstas no art. 11 da Lei, conforme o quadro abaixo:

BASE LEGAL	APLICABILIDADE	
	DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS
FORNECIMENTO DE CONSENTIMENTO PELO TITULAR	Sim	Sim
CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR	Sim	Sim
REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA	Sim	Sim
EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO	Sim	Não

Considerações Iniciais

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL	Sim	Sim
PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO	Sim	Sim
ATENDIMENTO AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO	Sim	Não
PROTEÇÃO DO CRÉDITO	Sim	Não
EXECUÇÃO DE POLÍTICAS PÚBLICAS PELA ADMINISTRAÇÃO PÚBLICA	Sim	Sim
GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR EM PROCESSOS DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE CADASTRO*	Não*	Sim
TUTELA DA SAÚDE EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA	Sim	Sim

** Note-se que as situações abarcadas na base legal do art. 11, II, g (garantia da prevenção à fraude e à segurança do titular em processos de identificação e autenticação de cadastro) poderiam estar cobertas pela base legal do legítimo interesse (art. 7º, IX) caso os dados não fossem sensíveis. Assim, não existe propriamente uma base legal "autônoma" capaz de legitimar somente o tratamento de dados sensíveis e não os demais.*

Considerações Iniciais

Dada a importância fundamental do estabelecimento da base legal para a legitimidade do tratamento de dados pessoais, cumpre um detalhamento sobre as mais frequentemente utilizadas:

- **Consentimento.** Utilizado quando o titular dos dados, livremente, autoriza que seus dados sejam tratados. Para que o consentimento seja válido, é necessário que o titular possua, previamente, todas as informações relevantes sobre como seus dados serão tratados, para que possa decidir de forma livre e informada se concorda com elas ou não. Caso concorde, o titular deve manifestar essa permissão de modo que não deixe margem a dúvidas sobre sua intenção.

- **Obrigação legal ou regulatória.** Diversas leis e regulamentos exigem que os dados pessoais do indivíduo sejam tratados, como, por exemplo, em obrigações de armazenamento de documentos tributários (como notas fiscais) por um certo período, assim como na guarda de dados de motoristas para o Código Identificador da Operação de Transporte (CIOT) ou de exames toxicológicos periódicos, entre diversas outras.

- **Execução de contrato.** Quando o tratamento de dados pessoais for uma condição imprescindível para a execução de um determinado contrato que envolve o titular dos dados, a base legal para seu tratamento é a execução do contrato - desde que restrito aos dados necessários.

- **Exercício regular de direito em processo judicial, administrativo ou arbitral.** Dados pessoais podem ser relevantes em processos judiciais, administrativos ou arbitrais, principalmente no que se refere à produção de provas. Essa é a base legal mais indicada quando o objetivo é utilizar os dados pessoais do titular no exercício de direitos dentro de um processo.

- **Legítimo interesse do controlador ou de terceiro.** Esta base legal, que não descreve uma conduta específica, é usada em situações variadas, nas quais o controlador pretende realizar um tratamento, de interesse seu ou de terceiro, que não afete de forma concreta e relevante os direitos

dos titulares dos dados tratados - por exemplo, ao promover os seus serviços e realizar iniciativas que beneficiem o titular de dados com utilização mínima, transparente e segura de seus dados pessoais. Um exemplo de sua adoção é o tratamento de dados pessoais para algumas modalidades de marketing direto ou o tratamento de dados para garantir a segurança de uma rede pública de wi-fi - sempre ressaltando que cada situação deve ser analisada e documentada particularmente e que, em várias circunstâncias, será recomendável elaborar Relatório de Impacto à Proteção de Dados Pessoais.

- **Proteção ao crédito.** Quando os dados pessoais forem utilizados para verificar a capacidade de adimplemento do titular em procedimentos de proteção ao crédito, essa base pode ser utilizada.

- **Garantia da prevenção à fraude.** O tratamento de dados sensíveis para a segurança em processos de identificação e autenticação de cadastro para evitar fraude é possível por meio desta base legal, que legitima, por exemplo, a utilização de dados biométricos como elemento de identificação.

É importante destacar que tanto as bases legais quanto os princípios anteriormente destacados devem sempre ser levados em consideração para confirmar a legitimidade e a compatibilidade de uma operação de tratamento de dados pessoais à luz da LGPD.

No setor de transporte, merecem especial atenção, entre outras, as bases legais (i) de execução de contrato ou de procedimentos preliminares relacionados a contrato e (ii) de cumprimento de obrigação legal ou regulatória pelo controlador, entre outras. A primeira porque é bastante comum em virtude da própria prestação do serviço de transporte, a segunda em virtude da extensa legislação setorial em vigor, especialmente as normativas das agências reguladoras dos modais de transporte, sejam elas a Agência Nacional de Aviação Civil (ANAC), a Agência Nacional de Transportes Terrestres (ANTT) e a Agência Nacional de Transportes Aquaviários (ANTAQ).

Considerações Iniciais

1.2.4. DIREITOS DOS TITULARES

A LGPD atribui aos titulares de dados a possibilidade de exercer uma série de direitos, que podem ser postulados perante os controladores. Os direitos do titular de dados estão previstos nos arts. 18 a 22 da LGPD e destacados no quadro abaixo:

- Confirmação da existência de tratamento dos dados pessoais (art. 18, I)
- Acesso aos dados pessoais (art. 18, II)
- Correção de dados pessoais incompletos, inexatos ou desatualizados (art. 18, III)
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV)
- Portabilidade dos dados pessoais a outro fornecedor de serviço ou produto (art. 18, V)
- Eliminação dos dados pessoais tratados com o consentimento do titular (art. 18, VI)
- Informação das entidades públicas ou privadas com as quais o controlador realizou uso compartilhado dos dados (art. 18, VII)
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII)
- Revogação do consentimento (art. 18, IX)
- Direito de oposição (art. 18, § 2º) ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, nos casos de violação da LGPD.

Considerações Iniciais

- **Solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses do titular (art. 20, *caput*)**

- **Obter informações claras e adequadas a respeito dos critérios e dos procedimentos utiliza-dos para a decisão automatizada, observados os segredos comercial e industrial (art. 20, § 1º)**

- **Informações sobre critérios utilizados para a decisão automatizada, observados os segredos comercial e industrial.**

Os controladores devem proporcionar aos titulares meios para o exercício de seus direitos, e a implementação dos procedimentos e sistemas necessários para tal é um elemento fundamental para a correta adequação de uma empresa ou organização à LGPD. Sistemas deste gênero se concretizam, por exemplo, pelo estabelecimento de um canal de comunicação que permita o exercício, pelos titulares, de seus direitos de forma gratuita e dentro dos prazos legalmente previstos.

Entre os direitos dos titulares, alguns costumam ser exercidos com maior frequência - e são referidos habitualmente como os direitos ARCO: são estes os direitos de (i) Acesso; (ii) Retificação (ou correção); (iii) Cancelamento (ou eliminação); e (iv) Oposição.

Ainda entre os direitos do titular, há aqueles referentes à requisição de informações que lhe devem ser fornecidas sobre o tratamento, seja aquela que deve ser previamente disponibilizada quanto na resposta a requerimentos sobre maiores detalhamentos de aspectos específicos do tratamento de seus dados.

Ainda em relação à informação, destaca-se também a previsão do art. 20, que estabelece dois direitos interconectados para a proteção do titular contra possíveis vieses decorrentes de decisões automatizadas, como o direito à explicação e o direito à revisão de decisões tomadas de forma automatizada.

O direito à explicação implica na obrigação de que o titular dos dados receba informações suficientes e inteligíveis para compreender suficientemente a lógica e os critérios utilizados para o tratamento dos seus dados, conforme previsão do § 1º. Já o direito à revisão abarca o direito do titular requisitar a revisão de uma decisão totalmente automatizada que afete os seus interesses, especialmente aqueles relacionados à definição do seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos da sua personalidade.

1.3. O TRATAMENTO DE DADOS PESSOAIS

Uma vez verificado o quadro geral que legitima o tratamento de dados pessoais, pelo seu enquadramento na devida base legal, pertinência aos princípios e à moldura conceitual da LGPD, passa-se a considerar o conjunto de dinâmicas que concretamente ocorrem durante o tratamento de dados pessoais para que se verifiquem as condições de legitimidade do tratamento de dados pessoais.

A LGPD é uma normativa permeada dos chamados deveres de conduta - isto é, um conjunto de procedimentos e ações que devem ser observados durante as operações de tratamento de dados. A não observância destes deveres de conduta pode implicar na inobservância do preceito legal e, em si próprio, gerar consequências jurídicas. Note-se, portanto, que a LGPD pode ser infringida, mesmo que não ocorra algo como um incidente de segurança ou uma violação explícita aos direitos dos titulares, já que a não observância das condutas que a lei prescreve, com o objetivo de diminuir os riscos no tratamento de dados, já implica no não cumprimento da lei, com consequências como sanções ou demandas judiciais.

Nesse sentido, é clara a necessidade de que em todas as fases do tratamento dos dados pessoais devem ser estritamente observados os preceitos legais pertinentes.

Destacaremos a seguir as principais situações nas quais estes preceitos pertinentes ao chamado ciclo de vida dos dados devem ser observados. Nos protocolos, presentes nos capítulos seguintes, diversas dessas situações serão objeto de maior aprofundamento.

Considerações Iniciais

1.3.1. AGENTES DE TRATAMENTO DE DADOS

Os tratamentos de dados pessoais são realizados somente por um dos agentes de tratamento, que a LGPD estabelece como o controlador ou o operador. A identificação de ambos é realizada a partir do enquadramento das atividades que este efetivamente realiza em relação aos dados pessoais, levando em conta os aspectos concretos do tratamento. Assim, o enquadramento de um agente de tratamento como controlador ou operador depende de aspectos concretos dos tratamentos de dados pessoais que este realiza, não sendo passível de ser realizado por autodeclaração, através de previsão contratual ou outro meio sem o aporte de elementos que levem em consideração a realidade do tratamento de dados.

As características de cada um dos agente de tratamento, que vão determinar o seu enquadramento, são as seguintes:

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais, definindo a sua finalidade, as principais características do tratamento e, quando for o caso, fornecendo ao operador as instruções para que este trate os dados segundo os parâmetros indicados. Em geral o controlador é o interessado no tratamento, embora esta não seja condição para a sua caracterização. Como responsável pela tomada de decisões acerca do tratamento, o controlador assume de forma ampla a responsabilidade pelo tratamento dos dados pessoais.

O operador é o agente responsável por realizar o tratamento de dados de acordo com as instruções e comandos do controlador e conforme a finalidade por este delimitada. Embora não seja uma exigência legal, na ampla maioria das ocasiões o operador é pessoa jurídica. Ele é, de todo modo, sempre uma pessoa distinta do controlador e somente será responsável em caso de inobservância das instruções do controlador ou quando não observe a Lei. Caso o controlador não terceirize o tratamento de dados pessoais, não haverá, em um dado tratamento, a figura do operador, dado que o próprio controlador realizará a totalidade das operações necessárias para o tratamento de dados.

Considerações Iniciais

A principal diferença entre o controlador e operador, a priori, é o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador. Ambos também diferem quanto ao regime de responsabilidade assumido que, em relação ao operador, é limitado. É exatamente por esse motivo que a correta definição dos papéis de tratamento na relação entre controlador e operador é essencial nas relações que envolvam tratamento de dados pessoais.

É importante ressaltar que o operador somente restará caracterizado quando houver a terceirização de tratamento de dados para uma pessoa que não seja o controlador. Nas ocasiões, muito frequentes, em que o próprio controlador realiza o tratamento, não há operador. Há, ainda, casos em que mais de um controlador está presente em uma operação de tratamento (quando há controladores conjuntos), casos em que o operador pode delegar a execução da sua tarefa para outro operador (quando se verifica a existência de um suboperador), ressaltando a necessidade de que se verifiquem os elementos objetivos do tratamento para estabelecer corretamente qual o papel de uma determinada empresa ou organização. A Autoridade Nacional de Proteção de Dados publicou, em maio de 2021, o seu "Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado" detalhando o tema[1].

Tanto o controlador quanto o operador, enquanto agentes de tratamento, devem cumprir com as diversas obrigações destacadas ao longo do texto da LGPD e, em particular, nos arts. 37 a 41, destacando-se, dentre elas: (i) a adoção de medidas de segurança, técnicas e organizativas para proteção dos dados pessoais; (ii) o registro das operações de tratamento de dados; (iii) a elaboração do Relatório de Impacto à Proteção de Dados Pessoais; (iv) a indicação do Encarregado de Dados, entre tantas outras.

1. Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf

1.3.2. ENCARREGADO PELO TRATAMENTO DE DADOS

O Encarregado pelo tratamento de dados é a pessoa indicada pelo controlador e operador que funciona como uma espécie de ponto focal para diversas dinâmicas em uma empresa ou organização referentes à aplicação da LGPD. Entre estas, estão a sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), cujas atribuições são: (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O encarregado deve ser indicado por toda empresa ou organização que realize o tratamento de dados pessoais, com a eventual exceção de casos que possam ser dispensados de sua indicação pela Autoridade Nacional de Proteção de Dados[1]. Os agentes de tratamento devem divulgar os contatos do encarregado publicamente.

1.3.3. SEGURANÇA DA INFORMAÇÃO

Especificamente quanto à segurança da informação, é importante destacar que os agentes de tratamento devem implementar 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, difusão ou qualquer forma de tratamento inadequado ou ilícito, adotando, sempre que possível, procedimentos e técnicas capazes de diminuir os riscos no tratamento, tal como o recurso à criptografia, a anonimização, a pseudonimização de dados pessoais, entre outros.

Contudo, caso ainda assim ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o controlador deve comunicá-lo à ANPD em prazo

1. No momento da finalização deste guia, a ANPD ainda não identificou casos de dispensa de indicação de encarregado.

razoável, mencionando (i) a descrição da natureza dos dados pessoais afetados; (ii) as informações sobre os titulares envolvidos; (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iv) os riscos relacionados ao incidente; (v) os motivos da demora, no caso de a comunicação não ter sido imediata; e (vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

1.3.4. TUTELA ADMINISTRATIVA E SANÇÕES

Conforme exposto, face aos deveres impostos pela LGPD aos agentes de tratamento de dados, seu descumprimento poderá ocasionar consequências negativas, seja financeiras ou reputacionais, para os agentes de tratamento.

Nesse aspecto, ressalta-se que os agentes de tratamento serão responsabilizados se, em razão do exercício do tratamento de dados pessoais, causem dano patrimonial, moral, individual ou coletivo aos titulares, conforme determinam os arts. 42 a 45 da LGPD. As sanções administrativas aplicáveis estão previstas logo em seguida, no art. 52 da Lei.

São elas, das mais brandas às mais onerosas: (i) advertência; (ii) multa simples, de até 2% do faturamento, limitada, no total, a cinquenta milhões de reais por infração; (iii) multa diária, observado o limite total de cinquenta milhões de reais; (iv) publicização da infração após devidamente apurada e confirmada a sua ocorrência; (v) bloqueio dos dados pessoais até a sua regularização; (vi) eliminação dos dados pessoais; (vii) suspensão parcial do funcionamento do banco de dados; (viii) suspensão do tratamento dos dados pessoais; ou (ix) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Nesse sentido, um importante parâmetro a ser observado para a aplicação gradativa, isolada ou cumulativa das sanções é a adoção de políticas de boas práticas e governança pelos agentes de tratamento. A LGPD recomenda que os controladores e operadores formulem regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos,

Considerações Iniciais

as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Para tanto, tais agentes devem sempre considerar, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, bem como a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento. Além disso, devem também demonstrar seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, das boas práticas estabelecidas.

Vale destacar que o cumprimento da LGPD pode ser fiscalizado por autoridades além da ANPD, tais como o Ministério Público e a Senacon (Secretaria Nacional do Consumidor), bem como pelos próprios titulares de dados, que poderão requerer indenizações por danos morais e materiais caso venham a sofrer danos em decorrência de tratamento inadequado de seus dados pessoais.

O presente Guia de Boas Práticas, que se enquadra justamente como um elemento fundamental para atender a recomendação legal e evidenciar a proatividade na implementação dos preceitos de proteção de dados, demonstra assim sua extrema relevância. Seu papel é fundamental ao facilitar a aplicação da LGPD pelo setor, proporcionar um espaço de autonomia para formulação consensual de procedimentos e práticas setoriais adequadas, conferir segurança jurídica e uniformidade ao cumprimento da Lei e ainda auxiliar as autoridades administrativas, em especial à ANPD, a aplicar a LGPD de forma pertinente a uma realidade setorial específica como a do transporte. Desta forma, concretiza-se o modelo de autorregulação previsto no art. 50 da LGPD, a fim de que a aplicação das diretrizes legais seja adaptada à realidade específica dos agentes de tratamento.

1.4. A APLICAÇÃO DA LGPD NO SETOR DE TRANSPORTE

O setor de transporte realiza habitualmente atividades de tratamento de dados de diversas naturezas, desde o cadastro do passageiro até o momento final da viagem do cliente. Os dados pessoais são usados ativamente, por exemplo, em sistemas inteligentes de bilhetagem e *check-in* em áreas como as de aeroportos ou estações, a fim de aumentar o fluxo eficiente de passageiros; para melhorar a eficiência dos sistemas de planejamento urbano e permitir o desenvolvimento de sistemas autônomos de tráfego; para melhorar o setor de serviços, compartilhando dados com empresas e organizações terceirizadas, como agências e empresas de publicidade, entre outras atividades.

De um lado, os dados pessoais permitem que as empresas se tornem mais sofisticadas, eficientes e lucrativas e, de outro, permitem que os usuários do sistema de transporte (passageiros) se beneficiem do setor de forma mais rápida, barata e personalizada. A transformação tecnológica aumentou significativamente o uso e o compartilhamento de dados pessoais entre empresas. Exatamente por isso é fundamental que todo o setor de transporte se adeque às diretrizes da LGPD, a fim de garantir a plena conformidade de todas essas atividades.

Para uma melhor compreensão dos impactos da LGPD nos processos, fluxos e procedimentos do setor de transporte, bem como dos conceitos anteriormente abordados nos itens 1.2 e 1.3 deste Guia de Boas Práticas, confira o exemplo a seguir:

Considerações Iniciais

>> EXEMPLO 2

DA COMPRA DA PASSAGEM AÉREA ATÉ A CHEGADA AO DESTINO FINAL

Imagine uma situação na qual uma pessoa que mora no Rio de Janeiro precisa realizar uma viagem de trabalho a São Paulo. No site da companhia aérea escolhida, para realizar a compra da passagem, ela fornece diversos dados pessoais, informando seu nome completo, data de nascimento, telefone, e-mail, número de CPF (ou RG, CNH, passaporte), endereço residencial, CEP, informações financeiras (número do cartão de crédito, por exemplo) e, por vezes, até dados pessoais sensíveis (como nos casos em que o passageiro possua alguma doença específica que exija atendimento e acompanhamento individual durante o voo).

No dia do voo, o passageiro se dirige ao aeroporto e, no totem de autoatendimento, realiza o seu check-in, onde, mais uma vez, são coletados diversos dados pessoais, inclusive de terceiros, como nos casos de inclusão de um contato de emergência, a partir do nome completo e telefone de contato da pessoa. Novos dados pessoais são tratados caso o passageiro queira despachar a bagagem e certamente no momento em que ele ingressa na aeronave.

Após a chegada ao seu destino, os seus dados pessoais continuam sendo utilizados pela companhia aérea para avaliar os hábitos de voo, a fim de oferecer ofertas personalizadas, e também para coleta de feedback, ou seja, para que o passageiro avalie a sua experiência com a empresa.

Caso esse passageiro, por ter gostado muito da companhia aérea, torne-se cliente de categoria VIP, provavelmente ele receberá um cartão personalizado que, para ser impresso, exige o compartilhamento dos dados pessoais com a gráfica contratada pela companhia aérea e, por vezes, com a transportadora que realizará a entrega do cartão na residência deste passageiro.

Neste exemplo hipotético, utilizando os conceitos abordados anteriormente, o passageiro é o titular dos dados (já que as informações se referem a ele, ou seja, identificam-no) e a companhia aérea é o controlador (já que é ela que toma as decisões a respeito do tratamento que é realizado com estes dados pessoais). A gráfica e a transportadora, por sua vez, são operadores especificamente quanto à prestação de serviços respectivamente de impressão e transporte de cartões fidelidade da companhia aérea para os seus clientes VIP.

A partir do exemplo acima, que faz parte da rotina dos prestadores de serviço de transporte aéreo, mas que pode ser também adaptado aos outros modais de transporte, diversas outras questões podem ser suscitadas: em quais momentos os dados do passageiro (titular) foram tratados ao longo de toda a viagem? O compartilhamento das informações do passageiro com fornecedores e demais prestadores de serviço precisa do seu consentimento? Em que momento os dados do passageiro devem ser excluídos pelos agentes de tratamento?

A aplicação da LGPD requer uma análise detalhada de cada uma dessas questões e de muitas outras operações de tratamento de dados para que se atinja o objetivo de fornecer segurança aos passageiros, às empresas e aos cidadãos. Neste Guia de Boas Práticas serão abordadas diversas situações comuns no cotidiano do setor de transporte nas quais ocorre o tratamento de dados pessoais, com a indicação de procedimentos e posturas que podem auxiliar a plena efetivação dos ditames da LGPD no setor de transporte.

1.5. NATUREZA E ÂMBITO DE APLICAÇÃO DO GUIA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS NO SETOR DE TRANSPORTE

O presente Guia de Boas Práticas de Proteção de Dados Pessoais abrange as atividades do tratamento de dados pessoais realizadas por prestadores de serviços de transporte de passageiros e de cargas, bem como de serviços de logística e infraestrutura para transporte.

A Lei Geral de Proteção de Dados prevê, em seu art. 50, a possibilidade da formulação de regras de boas práticas em proteção de dados. Essa oportunidade se apresenta com o objetivo de proporcionar ao setor de transporte elementos que facilitem a interpretação e implementação da LGPD de forma mais prática, transparente e eficiente, ao analisar e detalhar aspectos da aplicação da Lei à realidade do setor, levando em conta as suas características específicas.

>> CAPÍTULO 1

Considerações Iniciais

Considerando que a LGPD é uma lei geral, aplicável indistintamente a todos os setores quando estes realizam tratamentos de dados pessoais, ela, naturalmente, não almeja tratar de particularidades de cada um desses setores, senão fornecer uma disciplina capaz de se adaptar às diversas realidades e situações de cada um. Reconhecendo a necessidade e valor de uma leitura das regras gerais da LGPD a partir das especificidades do setor de transporte, um dos objetivos deste Guia de Boas Práticas é a melhor visualização de como as normas gerais da LGPD serão efetivadas na realidade do setor, o que é útil não somente para as empresas de transporte como para os reguladores e autoridades públicas, que poderão contar com uma perspectiva da aplicação da Lei já adaptada ao setor.

Sendo este Guia de boas práticas composto de critérios, procedimentos e recomendações de caráter objetivo a respeito do tratamento de dados pessoais por empresas e organizações do setor de transporte, demonstra-se pertinente a subsequente elaboração de mecanismos de verificação e supervisão da efetividade das medidas nele previstas pelo setor. Este mecanismo, que funciona para promover e garantir a efetividade da proteção de dados e proporcionar a confiança dos usuários no ecossistema de transporte como um todo, poderá levar em consideração parâmetros e diretrizes internacionais, tais como as estabelecidas por autoridades de proteção de dados, bem como mecanismos análogos de supervisão de normas deontológicas e de autorregulação de entidades brasileiras.

Também de extremo relevo é a consideração de mecanismos e procedimentos de atualização deste Guia de Boas Práticas de Proteção de Dados, levando em conta o desenvolvimento da disciplina da proteção de dados no Brasil e a sua implementação, considerando tanto a evolução natural da matéria em si, a efetiva implementação da normativa deste Guia pelas empresas e organizações do setor, bem como novas regulamentações, diretrizes e precedentes que venham a ser produzidos por órgãos administrativos como a ANPD, ANTT, ANTAQ, ANAC, entre outros.

O Guia foi elaborado por um comitê formado por representantes dos diversos modais de transporte, auxiliado por especialistas na área de proteção de dados e teve sua redação coordenada pelo Sistema CNT (CNT/SESTSENAT/ITL).

>> CAPÍTULO 1

Considerações Iniciais

A missão da CNT é promover e garantir que o transporte cresça de forma segura, estratégica e sustentável. Hoje, a Confederação Nacional do Transporte é composta por 27 federações, 05 sindicatos nacionais e 21 entidades associadas. Isso representa mais de 155 mil empresas de todos os modais de transporte (rodoviário, ferroviário, navegação e aéreo), responsáveis pela geração e manutenção de mais de 2,2 milhões de empregos. Na composição do Sistema CNT, a instituição também administra o SEST SENAT (Serviço Social do Transporte e Serviço Nacional de Aprendizagem do Transporte) e o ITL (Instituto de Transporte e Logística).

O SEST SENAT está presente em todas as regiões do Brasil com 159 Unidades Operacionais equipadas para realizar atendimentos de saúde (nas áreas de odontologia, fisioterapia, psicologia e nutrição), ações de esporte e lazer e cursos para o desenvolvimento dos profissionais do transporte, seus familiares e da comunidade em geral. Já o ITL tem a missão de promover a geração do conhecimento, o aprimoramento do capital humano e a competitividade do setor de transporte através de cursos executivos nacionais e internacionais para os gestores das empresas.

>> CAPÍTULO 2

Protocolos Gerais

2.1. PROTOCOLO DE TRANSPARÊNCIA

A transparência de uma empresa ou organização em relação às operações de tratamento de dados que realiza é um dos princípios norteadores da LGPD e também elemento fundamental para a construção de uma relação de confiança junto aos titulares de dados.

Ao contribuir para a legitimidade dos tratamentos de dados, a estruturação adequada dos recursos de transparência é, igualmente, fator que pode otimizar o direcionamento de recursos para o atendimento de eventuais requisições pelos titulares, bem como para diminuir o volume de eventuais procedimentos administrativos e judiciais relacionados à proteção de dados.

A observância de práticas de transparência não se resume à disponibilização de determinados documentos, como políticas de privacidade, porém envolve todos os meios de comunicação e interação com titulares de dados, clientes e parceiros em geral. A amplitude da legislação a ser considerada, incluindo a Lei de Acesso à Informação e o Código de Defesa do Consumidor nos casos aplicáveis, atesta a necessidade de que sejam utilizados todos os meios hábeis disponíveis, a fim de fornecer canais de comunicação que sejam adequados para a promoção da transparência sobre as operações de tratamento de dados.

I. **A transparência sobre as operações de tratamento de dados pessoais deve ser concretizada a partir da utilização tanto de instrumentos que informem sobre tratamentos específicos de dados pessoais, mediante requisição de informações pelos respectivos titulares, como de instrumentos de caráter geral, como políticas de privacidade e comunicações variadas, que informem sobre as principais características dos tratamentos realizados, para os casos em que este conhecimento seja relevante para terceiros como, por exemplo, para potenciais clientes ou usuários dos serviços da empresa ou organização.**

Protocolos Gerais

II. As empresas e organizações devem implementar, em suas operações de tratamento, procedimentos que facilitem a identificação e o fornecimento ao titular dos dados, mediante requisição deste, das informações referidas no artigo 9º, I a VII, da LGPD, quais sejam: a finalidade específica do tratamento; a forma e duração do tratamento, observados os segredos comercial e industrial; a identificação do controlador; as informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e os direitos do titular, com referência aos direitos presentes no artigo 18º da LGPD.

III. As empresas e organizações devem avaliar se existem outras informações que possam ser consideradas relevantes sobre o tratamento para os titulares nos tratamentos que realizem, a fim de lhes garantir a clareza e o conhecimento necessário em relação aos aspectos principais do tratamento, ainda que não estejam incluídas entre as informações referidas no artigo 9º, I a VII da LGPD.

IV. As características gerais dos tratamentos de dados realizados por empresas e organizações devem ser divulgadas de forma ampla, por meio de instrumentos como políticas de privacidade, aviso de privacidade, termos de uso, FAQ (questões frequentemente perguntadas) e outros similares que cumpram a função de tornar públicos, ou de conhecimento prévio pelos potenciais interessados, os aspectos fundamentais do tratamento de dados.

V. Em razão das características, volume das operações e da demanda por informações sobre o tratamento de dados pessoais em determinada empresa ou organização, estas poderão ter sua disponibilização centralizada em um Portal de Privacidade, ou mecanismo semelhante, disponível em meio digital e que facilite o acesso dos titulares à informação e à documentação referente ao tratamento de seus dados, bem como proporcione ferramentas para facilitar

Protocolos Gerais

a requisição de informações específicas sobre determinados tratamentos, podendo ainda concentrar outros aspectos do relacionamento com o titular, incluindo o exercício dos seus direitos e outras funções pertinentes.

VI. As informações sobre o tratamento de dados pessoais de empregados e prestadores de serviço devem ser disponibilizadas de forma clara e facilitada pelas empresas e organizações por meio de instrumentos como portais internos para empregados e colaboradores e similares, que poderão permitir igualmente a requisição por estes de informações sobre tratamentos específicos.

VII. A empresa ou organização poderá, dependendo do volume e natureza dos dados pessoais que trate, elaborar um plano de comunicação interno com informações sobre o tratamento de dados de empregados e prestadores de serviço, que será periodicamente atualizado para garantir a sua efetividade e a pertinência dos dados.

VIII. O fornecimento de informações sobre o tratamento de dados pessoais aos titulares de dados deverá ser garantido de forma ampla, clara e precisa, ou seja, a partir de uma linguagem simples, não rebuscada, que indique exaustivamente todas as informações relevantes, evitando-se termos genéricos e ambíguos. Deve, ainda, considerar a necessidade do atendimento aos interesses dos titulares, sendo que as eventuais restrições ao fornecimento de informações com base na proteção do segredo estratégico, industrial e comercial deverão ser justificadas e restritas somente às informações imprescindíveis para a sua manutenção.

Protocolos Gerais

A seguir, mencionamos alguns exemplos de práticas que podem ferir o princípio de transparência e possíveis soluções:

EXEMPLO 1	**PROBLEMA: Constar na Política de Privacidade que a coleta dos dados pessoais tem a finalidade genérica de "melhorar a experiência do titular no uso da aplicação".** **POSSÍVEL SOLUÇÃO:** Mencionar de que forma e com quais dados e modalidades de tratamentos a experiência do titular poderá melhorar.
EXEMPLO 2	**PROBLEMA:** Constar na Política de Privacidade que os dados pessoais são compartilhados com parceiros para a finalidade meramente genérica, tal como "melhorar a experiência na aplicação e fornecer conteúdos personalizados" ou semelhante. **POSSÍVEL SOLUÇÃO:** Especificar de forma concreta e com o detalhamento necessário sobre a finalidade do compartilhamento de dados com parceiros.
EXEMPLO 3	**PROBLEMA:** Tratar os dados pessoais para finalidades não especificadas e informadas ao titular no momento da coleta. **POSSÍVEL SOLUÇÃO:** Somente realizar operações de tratamento de dados quando estas forem devidamente informadas ao titular na coleta, respeitando a finalidade especificada.
EXEMPLO 4	**PROBLEMA:** Utilizar linguagem excessivamente rebuscada e técnica para explicar ao titular dos dados acerca das características do tratamento. **POSSÍVEL SOLUÇÃO:** Disponibilizar meios de informação ao titular em linguagem acessível e informativa sobre o processo de tratamento de seus dados.

Protocolos Gerais

2.2. PROTOCOLO DE DIREITOS DO TITULAR

Os Direitos dos titulares de dados pessoais, especificados na LGPD nos seus artigos de 18 a 20, juntamente com os demais que se possam assumir de sua interpretação, devem ser garantidos pelos agentes de tratamento, podendo ser requeridos diretamente pelo titular ou seu representante a qualquer momento.

Os direitos dos titulares são:

- Confirmação da existência de tratamento de seus dados;
- Livre acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Portabilidade de dados;
- Eliminação dos dados tratados com base no consentimento;
- Informação sobre as entidades públicas e privadas com os quais houve compartilhamento dos dados pessoais;
- Informação sobre consequências de não fornecer o consentimento;
- Revogação de consentimento;

Protocolos Gerais

- Oposição;
- Não ter os dados pessoais referentes ao exercício regular de seus direitos utilizados em seu prejuízo;
- Revisão de decisões automatizadas;

No caso do não atendimento de uma requisição do titular de dados em relação aos seus direitos, ou no caso em que a resposta não for adequada, o titular poderá recorrer à Autoridade Nacional de Proteção de Dados, ao órgão de defesa do consumidor (caso a demanda também possa ser caracterizada como uma relação de consumo) ou mesmo ao Poder Judiciário para procurar obter a satisfação de sua demanda.

A disponibilização de mecanismos eficazes para que os titulares de dados possam exercer seus direitos é um dos elementos fundamentais para garantir a efetividade da LGPD, para o estabelecimento de uma relação de confiança com os titulares dos dados e, consequentemente, para a potencial diminuição de atritos e demandas administrativas ou judiciais por parte dos titulares de dados.

I. **As informações necessárias para que o titular possa exercer seus direitos, tais como contatos de responsáveis ou encaminhamento através de portais dedicados, deverão ser disponibilizadas publicamente e serem facilmente acessíveis para os titulares de dados, sempre incluindo as informações de contato do encarregado do tratamento de dados, quando este é indicado. No caso de operações de maior porte, ou volume de tratamento de dados, será dada preferência a métodos automatizados de requerimento dos direitos pelos titulares, tais como Portais de Privacidade ou semelhantes, que poderão centralizar o relacionamento com o titular dos dados, podendo incluir igualmente funções de transparência e outras que sejam pertinentes.**

Protocolos Gerais

II. **Os controladores de dados devem estabelecer procedimentos facilitados para o encaminhamento dos requerimentos dos direitos dos titulares, que deverão ser satisfeitos no menor tempo operacionalmente possível ou dentro do prazo de 15 (quinze) dias para a declaração completa, mencionada no art. 19, II da LGPD.**

III. **À medida em que prazos específicos sejam oportunamente regulamentados pela Autoridade Nacional de Proteção de Dados dentro de suas prerrogativas (LGPD, art. 18, §§ 4º e 5º), estes deverão ser contabilizados como limite máximo para satisfação do requerimento do titular, sendo que as empresas e organizações se empenharão no sentido de que os requerimentos sobre direitos que lhe sejam apresentados sejam encaminhados e respondidos no menor tempo operacionalmente possível, procurando promover a confiança e ressaltar a lealdade e boa-fé no tratamento de dados pessoais.**

IV. **Os controladores, nas ocasiões em que o tratamento de dados for efetivamente realizado pelo operador, segundo as suas instruções, deverão dispor de meios para que o operador possa lhe facilitar a satisfação dos requerimentos sobre direitos encaminhados pelos titulares. Estes meios incluem, entre outros, arranjos operacionais e contratuais.**

V. **As empresas e organizações devem verificar e autenticar a identidade dos titulares de dados que apresentem requisições de direitos. Para tal, devem empregar os meios necessários para proporcionar a segurança devida, que impliquem na coleta e tratamento de um mínimo de dados especificamente para fins desta autenticação e que não devem ser utilizados para outras finalidades, desde que não sejam dados pessoais já tratados anteriormente pela empresa ou organização.**

2.3. PROTOCOLO DE SENSIBILIZAÇÃO, CULTURA DE PROTEÇÃO DE DADOS E TREINAMENTO

A responsabilidade pelas operações de tratamento de dados é incumbência dos agentes de tratamento sendo, de fato, concretamente realizadas pelo conjunto de empregados e demais contratados. Atualmente, um volume razoável de atividades implica no tratamento, ainda que incidental, de dados pessoais, de onde deriva a necessidade de que noções básicas sobre proteção de dados pessoais sejam difundidas de forma horizontal entre o corpo de empregados e prestadores de serviço de uma empresa ou organização.

Esta difusão horizontal do conhecimento sobre o tema, que inclui ações de sensibilização, fortalecimento da cultura de proteção de dados e treinamento específico, conforme a necessidade de setores determinados, atende igualmente a vetores de responsabilidade social, ao proporcionar a todos os envolvidos nas operações da empresa ou organização acesso a informações relevantes sobre seus direitos.

Além disso, a difusão de informações relacionadas à proteção de dados dentro da organização está alinhada com os princípios norteadores da LGPD, mais especificamente os seus princípios da segurança e da prevenção, sendo que estas informações poderão ser eventualmente utilizadas como evidências caso a organização seja instada a comprovar a adoção de boas práticas em matéria de proteção de dados, em estrito cumprimento ao Princípio da Responsabilização e Prestação de Contas.

Para setores e categorias determinadas de empregados e prestadores de serviço que tenham importância estratégica, ou que realizem diretamente o tratamento de volume considerável de tratamento de dados pessoais, é ainda mais relevante a realização de treinamentos específicos, com atualização periódica, para que sejam proporcionados os instrumentos necessários para o desempenho de suas funções na estreita obediência da legislação e no respeito aos direitos dos titulares.

Protocolos Gerais

I. **Devem ser disponibilizadas a todos os empregados e prestadores de serviço de uma empresa ou organização informações sobre a importância da proteção de dados para a sua própria atividade e também para o cidadão, com o intuito de sensibilizá-los e chamar a atenção para a necessidade de atuação em conformidade com os ditames da legislação referente. A disponibilização desta informação poderá ser concretizada por meio de diversos instrumentos como guias, cartilhas, materiais que integrem "pílulas de conhecimento", palestras, ações de endomarketing e comunicação, divulgação de informações em site e redes sociais da empresa ou organização, criação de vídeos para integração de colaboradores e terceiros, elaboração de vídeos institucionais e campanhas diversas, bem como outros meios que se demonstrem eficazes.**

II. **O público-alvo das atividades de sensibilização, cultura de proteção de dados e treinamento abrange o universo de empregados e prestadores de serviço de uma empresa ou organização e poderá ainda incluir, a depender da necessidade e pertinência, colaboradores externos, parceiros e fornecedores, para que estejam cientes das práticas relacionadas à proteção de dados praticadas pela empresa ou organização.**

III. **Devem ser realizados treinamentos específicos para áreas críticas e estratégicas da empresa ou organização que realizem diretamente o tratamento de dados pessoais, como equipes de segurança da informação, recursos humanos, marketing, canais de atendimento como os Serviços de Atendimento ao Consumidor (SAC) e ouvidoria, bem como a sua alta direção. Esses treinamentos, conforme a necessidade, deverão ser virtuais ou presenciais, e deverão ser periodicamente atualizados. Empregados ou prestadores de serviço, conforme a necessidade, poderão igualmente ser inscritos em treinamentos externos.**

IV. **A empresa ou organização, conforme o volume de suas operações, poderá realizar a escolha ou indicação, entre os seus empregados ou prestadores de serviço, de pessoas que atuarão internamente como Embaixadores da Privacidade (Privacy Champions) ou semelhante – pessoas treinadas e capacitadas na área de proteção de dados que possam atuar como pontos de referência nas suas respectivas áreas para executar ações de engajamento e difusão de conhecimento sobre a matéria.**

V. **As atividades relacionadas à sensibilização, cultura de proteção de dados e treinamento devem abarcar não somente conteúdos relacionados à proteção de dados pessoais, mas também temas de segurança da informação, que deverão ser específicos conforme o volume e necessidade de cada empresa ou organização. Estas atividades poderão ser publicizadas e, necessariamente, devem ser registradas para a eventual necessidade ou pertinência de sua comprovação para fins de demonstração da adoção de boas práticas de governança mencionadas na "Seção II - Das Boas Práticas e da Governança" da LGPD e na realização das ações educativas mencionadas no artigo 50 da Lei.**

2.4. PROTOCOLO DE SEGURANÇA DA INFORMAÇÃO

Para garantir a segurança dos dados pessoais nas operações de tratamento, a LGPD exige que os agentes de tratamento adotem medidas de segurança preventivas e reativas, de caráter técnico ou administrativo, desde a concepção do produto ou do serviço (privacy by design, ou "privacidade na concepção") até a sua execução e durante todo o ciclo do tratamento das informações. Estas medidas, que não são detalhadas ou especificadas pela lei, devem ser de tal natureza que possam proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão ou qualquer outra forma de tratamento inadequado ou ilícito. Desta forma, contemplam o que é estabelecido pelos princípios da segurança e prevenção, previstos respectivamente no artigo 6º, VII e VIII da LGPD.

>> CAPÍTULO 2

Protocolos Gerais

As regras de segurança abrangem não somente o tratamento de dados em si, mas também a própria estruturação dos sistemas utilizados para tanto (artigo 49 da LGPD) e a obrigação de garantir a segurança da informação estende-se não apenas aos agentes de tratamento em sentido estrito, mas também a qualquer outra pessoa que intervenha em uma das fases do processamento de dados, mesmo após o seu término (artigo 47 da LGPD).

I. **Serão acompanhadas e implementadas as eventuais determinações a respeito de segurança da informação que sejam disciplinadas pela ANPD, a quem a LGPD, em seu artigo 46, § 1º, delega a competência de dispor sobre padrões técnicos mínimos de segurança da informação para o tratamento de dados. Paralelamente, as empresas e organizações podem adotar regras já consolidadas em programas de compliance ou em normativas técnicas específicas relacionadas à segurança da informação, tais como, por exemplo, normas e certificações da Associação Brasileira de Normas Técnicas (ABNT) ou da International Organization for Standardization (ISO), entre outras que se demonstrem pertinentes e adequadas para a garantia da segurança da informação e que sejam adotadas pelo mercado, inclusive no setor de transporte.**

II. **Além das medidas de caráter técnico, as empresas e organizações devem adotar também medidas de natureza administrativa, a partir da adaptação de rotinas de trabalho, de procedimentos de segurança da informação específicos e de mecanismos de transparência e governança de dados, mediante a estruturação de um programa de compliance que defina critérios padrão a serem adotados por toda a empresa ou organização. As técnicas e medidas adotadas devem ser proporcionais ao risco e a natureza dos dados pessoais tratados e ao contexto do tratamento, de acordo com a tecnologia comercialmente acessível e razoável para aquele determinado momento.**

Protocolos Gerais

III. As empresas e organizações devem adotar medidas específicas para controle de acesso lógico e físico quanto aos dados pessoais tratados, que sejam adequadas ao volume de suas operações, podendo incluir, por exemplo, registros de acesso, a utilização de sistemas automatizados de gestão de identidade e de restrição de permissões e controle de credenciais para aceder a arquivos físicos e setores específicos na sede da empresa ou organização onde constam bases de dados. Para melhor controle, devem ser instituídas regras internas sobre liberação de acessos, bem como sobre circulação e compartilhamento interno de dados pessoais de permissão de uso aos sistemas, a fim de adequar as permissões de acordo com as funções e responsabilidades de quem tem acesso aos dados pessoais.

IV. As empresas e organizações devem oferecer treinamentos contínuos e periódicos sobre segurança da informação e privacidade para colaboradores, parceiros, fornecedores, prestadores de serviço e demais envolvidos, de forma a consolidar uma cultura interna de segurança da informação e proteção de dados que estimule o cuidado constante com os dados pessoais tratados em todas as dimensões de seu tratamento. Caso seja viável, recomenda-se a elaboração ou compartilhamento de cartilhas, manuais, livretos ou afins para documentar internamente o conteúdo do treinamento, que poderão então ser utilizados pelos envolvidos sempre que necessário e, em caso de dúvidas, também nas atividades realizadas diariamente. Do mesmo modo, recomenda-se que sejam aplicadas metodologias para verificar a compreensão do conteúdo abordado nos treinamentos, inclusive pela adoção de planos de capacitação a partir dos resultados dos testes aplicados.

V. Com o objetivo de evitar ao máximo a ocorrência de incidentes de segurança e vazamentos de dados, e diminuir os riscos envolvidos, as empresas e organizações devem adotar práticas e sistemas de prevenção de perda de dados (Data Loss Prevention), garantindo a continuidade da base de dados da empresa ou organização, visando especialmente que dados confidenciais ou críticos permaneçam disponíveis apenas para usuários autorizados, impedindo que sejam

acessíveis para usuários não autorizados. Para tanto, é fundamental a adoção de mecanismos como: backups periódicos, armazenamento dos dados em fitas, utilização de VPN e criptografia, bem como adoção de medidas de segurança da informação específicas como firewall e antivírus, entre outras.

VI. No caso em que ocorra um incidente de segurança, as empresas e organizações devem realizar uma avaliação de risco, a fim de identificar potenciais impactos aos titulares de dados envolvidos, bem como notificá-los à ANPD, quando for o caso, ou seja, quando estes acarretarem risco ou dano relevante aos titulares. Para tanto, recomenda-se que sejam implementados protocolos específicos de gestão de incidentes de segurança e vazamentos de dados, com a formação de grupos de colaboradores com a função de gerenciar eventual crise no caso de consumação de incidente de segurança.

É recomendável a estruturação de grupos destinados a proporcionar estratégias a serem seguidas e respostas rápidas em casos de incidentes de segurança, no formato de um comitê de crise corporativo ou assemelhado, que pode ser formado por áreas multidisciplinares para tratar da gestão de incidentes de dados pessoais. Deve-se também garantir o funcionamento dos sistemas de logs dos servidores, como forma de garantir a rastreabilidade de acessos, além da implementação dos recursos técnicos de segurança da informação aptos a garantir os dados pessoais na medida de sua natureza e do risco que um incidente possa representar aos seus titulares.

Além disso, é indispensável que as empresas e organizações levem em consideração à regulamentação da ANPD sobre o tema, à medida que esta seja divulgada e atualizada, a fim de estarem continuamente em conformidade, levando em conta, nesta área, a tendência das atualizações acontecerem com razoável frequência.

Protocolos Gerais

VII. Para centralizar as regras instituídas quanto à segurança da informação, as organizações e empresas devem elaborar sua Política Interna de Segurança da Informação e Proteção de Dados, bem como os demais documentos que se façam necessários. Esta política poderá conter, dentre outras previsões, aspectos gerais sobre guarda e armazenamento de dados, prazos de retenção, mecanismos para registro de evidência de descarte de dados, procedimentos de backup, recomendações gerais para não exposição de informações, entre outras questões pertinentes. Tal documento deverá ser ampla e periodicamente divulgado internamente para os colaboradores, bem como encaminhado para parceiros, fornecedores, prestadores de serviço e outros terceiros, com a indicação de um canal de comunicação para esclarecimento de dúvidas e envio de reclamações.

VIII. Recomenda-se que as empresas e organizações utilizem as técnicas que restrinjam os danos e prejuízos decorrentes de eventuais incidentes de segurança, tais como as de pseudonimização e anonimização, ou que mantenham a informação pessoal armazenada em formato criptografado. Para tanto, devem ser utilizados os meios técnicos razoáveis e disponíveis na ocasião do tratamento dos dados, considerando, especialmente no caso da anonimização, fatores objetivos, como custo e tempo necessários para reverter o processo de acordo com as tecnologias disponíveis, além da utilização exclusiva de meios próprios. Nesse caso, as regras previstas na LGPD passam a incidir imediatamente, assim como já incidem no caso do tratamento de dados pseudonimizados.

IX. Nos casos de compartilhamento de dados pessoais pelos controladores com operadores e suboperadores, bem como nos casos de controladores conjuntos, recomenda-se que sejam desenvolvidos mecanismos e protocolos específicos para realização de auditorias pontuais e periódicas nos sistemas de terceiros que estejam envolvidos no tratamento, bem como nas medidas organizacionais e técnicas utilizadas no tratamento de dados pessoais, a fim de verificar, avaliar e confirmar que tais sistemas seguem os parâmetros mínimos de segurança da informação e proteção de dados estabelecidos pela empresa ou organização.

2.5. PROTOCOLO DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência de dados pessoais para fora do território nacional implica na necessidade de que medidas preventivas necessárias sejam tomadas para que se evite que esta, de alguma forma, implique no enfraquecimento ou relativização das garantias dos titulares de dados. A elaboração de uma normativa de alcance nacional deve, necessariamente, incluir mecanismos que definam parâmetros e limites para a transferência de dados para fora do território nacional, que devem ser observados.

A transferência internacional é, em determinadas ocasiões, útil ou mesmo imprescindível para a atividade de transporte, sendo uma realidade inafastável em uma economia globalizada. É necessária, portanto, a verificação de parâmetros adequados para que essas transferências sejam realizadas de forma legítima, em consonância com a legislação e sem ferir direitos e expectativas legítimas dos titulares de dados.

Parcela relevante dos instrumentos e critérios necessários para a definição dos parâmetros para a transferência internacional de dados ainda depende de definições e de regulamentação a ser futuramente produzida pela Autoridade Nacional de Proteção de Dados (ANPD). Assim, além da necessidade de participação nas discussões sobre estas definições e da sua implementação, quando ocorrerem, mostra-se pertinente a adoção de procedimentos para a transferência internacional de dados que procure atender aos parâmetros gerais da LGPD e que estejam em sintonia com parâmetros internacionalmente reconhecidos.

I. **As transferências de dados pessoais para fora do território nacional serão identificadas e avaliadas de acordo com a sua necessidade, devendo ser realizadas somente quando necessárias, justificadas e adequadas em relação à finalidade pretendida.**

Protocolos Gerais

II. Nas transferências internacionais de dados pessoais autorizadas pelo consentimento do titular, este deverá ser obtido de forma específica, apartado de outras cláusulas contratuais e com destaque para a transferência, com informação acerca do caráter internacional da operação e de outras informações que sejam relevantes no contexto da transferência.

III. Os contratos de transporte cuja execução implique na transferência internacional de dados serão redigidos de forma a tornar claros os principais elementos desta transferência, tais como as categorias de dados transferidos, os destinatários e a finalidade, bem como para assegurar ao titular conhecimento facilitado sobre a transferência e seus aspectos principais.

IV. As empresas e organizações do setor de transporte considerarão a pertinência da formulação de cláusulas contratuais modelo para a transferência internacional de dados pertinentes ao setor de transporte ou a modais específicos.

V. Será considerada, em contratos que impliquem a transferência internacional de dados, a inclusão de cláusulas padrão que forneçam ao titular a garantia de que o nível de proteção no país de destino dos dados será equivalente ao proporcionado pela LGPD, bem como de especificações sobre o tratamento de dados pessoais que sejam reconhecidas por Autoridades de Proteção de Dados de outros países, até o momento em que a Autoridade Nacional de Proteção de Dados vier a elaborar seu próprio modelo de cláusulas padrão.

VI. Será levada em consideração a adoção de medidas de certificação referentes à adoção de práticas e medidas para garantir a integridade e segurança na transferência internacional de dados oferecidas por instituições idôneas e reconhecidas em sua área de atuação.

VII. **As transferências internacionais de dados que sejam, total ou parcialmente, homologadas e legitimadas perante autoridades de proteção de dados de outros países podem ser documentadas e publicizadas como fator indicativo da proatividade na matéria até que sejam editadas as regulamentações que possibilitem a ampla utilização das diversas hipóteses permissivas da transferência internacional de dados previstas na LGPD.**

VIII. **No caso de empresas ou organizações com atuação em diversos países, será considerada a formulação ou adesão a cláusulas corporativas globais, que definirão as práticas e procedimentos relacionados ao tratamento de dados pessoais dentro de uma determinada empresa ou organização independente do país nos quais se encontrem os dados pessoais, que deverão observar nível de proteção aos direitos do titular equivalente ao proporcionado pela LGPD.**

2.6. PROTOCOLO DE MARKETING

Com o advento da LGPD, atividades de marketing que se utilizam de dados pessoais para direcionar mensagens publicitárias (como no caso do marketing direto), pesquisas de marketing e outras modalidades de tratamento de dados pessoais com fins de oferecimento de produtos ou serviços, passam a estar sujeitas aos parâmetros da legislação de proteção de dados.

Considerando que o marketing é uma atividade que visa aproximar o mercado de seus pólos de demanda mais específicos e potencializar as relações econômicas, a atividade está relacionada diretamente a alguns dos fundamentos da Lei Geral de Proteção de Dados no que se refere ao desenvolvimento econômico e à livre iniciativa. Assim, os tratamentos de dados pessoais para atividades relacionadas ao marketing podem se desenvolver dentro de um espaço de legitimidade, observando os direitos e garantias dos titulares em relação aos seus dados pessoais e incorporando medidas para promover a transparência e facilitar o exercício de direitos pelos titulares.

Protocolos Gerais

I. As comunicações realizadas para finalidade de marketing que utilizam dados pessoais para direcionamento a um determinado perfil ou público-alvo deverão ser identificadas como tal e possuir mecanismo que permita ao destinatário revogar o consentimento fornecido para o recebimento da comunicação, quando esta for a base legal utilizada, ou para que ele opte pelo não recebimento de posteriores comunicações deste gênero quando o tratamento dos dados tiver outra base legal. Em ambas as hipóteses o mecanismo deve proporcionar a cessação das comunicações de forma facilitada e eficaz.

II. Será avaliada a adoção de mecanismos desenvolvidos e disponibilizados por associações e entidades que possam facilitar a identificação de opções no sentido de receber comunicações de marketing direto sobre determinados assuntos, ou não as receber, como no caso de mecanismos de optout tools ou similares, desde que referidos mecanismos demonstrem-se eficazes.

III. Nos processos que envolvam ações de marketing direcionado devem ser tratados somente os dados estritamente necessários, evitando-se assim o tratamento de dados em excesso.

IV. O tratamento de dados pessoais para fins de marketing preferencialmente não será integrado ao tratamento de dados pessoais cadastrais ou outros utilizados pela empresa ou organização para outras finalidades. Quando isto se demonstrar pertinente, por interesses da empresa ou mesmo dos titulares ou terceiros, recomenda-se realizar a avaliação de legítimo interesse (LIA - Legitimate Interest Assessment) ou , conforme seja pertinente a elaboração de Relatório de Impacto à Proteção de Dados com o fim de minimizar os riscos envolvidos, em particular nos casos em que a coleta de informações de marketing seja integrada à coleta de dados identificativos dos titulares.

Protocolos Gerais

V. Nos casos em que a atividade de tratamento de dados para fins de marketing se fundamente em processos automatizados será necessário garantir que a atividade não se faça uso de qualquer critério discriminatório.

VI. Em todo caso de utilização de dados pessoais para fins de marketing será dada ampla publicidade e transparência ao tratamento, através de instrumentos que sejam pertinentes como, por exemplo, o aviso de cookies, aviso de privacidade em destaque em sites e aplicações, bem como a presença da informação necessária nos diversos meios de contato e de comunicação com os titulares.

VII. Nos casos de compartilhamento de dados pessoais com empresas parceiras, como agências de publicidade, para a realização de atividades de marketing digital e mídia programática, é necessário assegurar-se que estas estejam com seus processos adequados à LGPD, assim como os respectivos instrumentos contratuais pactuados prevejam responsabilidades de cada agente, padrões de conduta e procedimentos a serem adotados em casos de incidentes de segurança.

VIII. Nos casos de endomarketing e marketing institucional, nos quais eventualmente sejam utilizadas imagens ou voz de titulares que sejam colaboradores da empresa ou organização, seus dependentes ou de clientes, é necessária a obtenção de consentimento específico para o uso e para o compartilhamento de dados. Na utilização de dados de crianças e adolescentes para campanhas específicas deverá ser obtida autorização específica e em destaque, fornecida por, ao menos, um dos pais ou responsável legal, sempre observando o seu melhor interesse.

IX. Quando for necessária a coleta de dados pessoais para caracterização do público na realização de pesquisas de marketing deverão ser tratados somente os dados estritamente necessários para a realização da finalidade pretendida pela pesquisa, desde que a divulgação da pesquisa não permita a identificação dos participantes.

X. **Quando houver necessidade de contratação de empresas para a realização das campanhas, pesquisas, elaboração de material, deve-se zelar para que o respectivo contrato seja redigido de forma a garantir a conformidade da atividade de marketing com a LGPD e outras legislações aplicáveis.**

2.7. PROTOCOLO PARA TRANSPORTE DE PASSAGEIROS

Na atividade de transporte de passageiros é necessária a utilização de informações pessoais para a própria execução do contrato. Precisamente por ser esta modalidade de transporte centrada na pessoa, há diversas situações nas quais os dados de passageiros são necessários para o transporte ou são úteis para fins que vão desde a segurança do serviço, facilitação do uso, acessibilidade, combate a fraudes, melhoria de sistemas de atendimento ou mesmo da própria infraestrutura de transporte, entre outras.

Considerando a multiplicidade de situações nas quais os dados pessoais de passageiros podem vir a ser tratados, este protocolo procurará abranger as situações mais relevantes no momento.

2.7.1. CADASTROS PARA COMPRA DE PASSAGENS E IDENTIFICAÇÃO DO PASSAGEIRO

A devida identificação do passageiro é condição necessária para a formalização do contrato de transporte de passageiros, o que autoriza a utilização de dados pessoais para esta finalidade. Além disso, dentro do espectro dos dados necessários para a realização deste contrato estão os dados pessoais utilizados para fins de cobrança, que podem ser referentes ao próprio passageiro ou a terceiro.

>> CAPÍTULO 2

Protocolos Gerais

I. Os dados pessoais necessários para a correta identificação do passageiro na execução de contrato de transporte serão somente aqueles imprescindíveis para que a atividade de transporte seja devidamente realizada e para que seja conferida a segurança necessária à prestação do serviço.

II. Os sistemas de venda de passagens serão concebidos e implementados de forma a proporcionar a máxima funcionalidade a partir da coleta dos dados estritamente necessários para permitir a prestação do serviço de transporte.

III. Tratamento de dados pessoais para finalidades relacionadas à melhoria do processo de venda, ao fornecimento de serviços personalizados ao passageiro ou similares, como programas de fidelidade, deverá ser informado de forma clara ao titular, que poderá, caso deseje, se opor à utilização de seus dados ou consentir com a sua utilização, a depender da base legal aplicada para o seu tratamento.

IV. Os procedimentos que utilizem dados pessoais para a detecção e prevenção de fraude serão precedidos de análise sobre seu impacto e risco para a proteção de dados pessoais, aos quais também será dada a transparência necessária. Os dados pessoais utilizados para estas finalidades serão coletados diretamente do titular ou de terceiros, e tratados exclusivamente para a finalidade de detecção e prevenção de fraude, com exceção de situações legalmente permitidas.

V. A utilização de dados pessoais de passageiros para finalidades relacionadas à realização de estatísticas, monitoramento de uso para melhoria e aperfeiçoamento do serviço e outras finalidades similares utilizarão, sempre que possível, dados anonimizados ou pseudonimizados.

2.7.2. TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

I. A utilização de dados pessoais sensíveis de passageiros será restrita às situações nas quais estes sejam indispensáveis para atividades relacionadas diretamente à prestação do serviço de transporte com segurança ou em casos expressamente previstos em lei, devendo-se evitar os tratamentos de dados sensíveis quando houver outros meios para que a mesma finalidade seja atingida a partir de dados pessoais não sensíveis.

II. A utilização de dados pessoais sensíveis com base no consentimento do titular será sempre precedida do amplo fornecimento de informações ao passageiro sobre a finalidade e características do tratamento de dados. Além disso, sempre que estes dados sensíveis não sejam necessários para a execução do contrato de transporte, deve ser oferecido ao passageiro uma verdadeira opção de aceitar ou recusar os termos propostos, ou recusá-los sem ser prejudicado, além da informação clara sobre as eventuais consequências caso não seja dado o consentimento.

III. Diante da natureza especial conferida às categorias de dados pessoais sensíveis, as empresas e organizações devem dar prioridade à sua proteção, eis que eventuais incidentes relacionados a estes dados têm o potencial de afetar de forma mais significativa e crítica os direitos e a esfera de privacidade dos titulares. Assim recomenda-se, no tratamento destas informações, que sejam garantidos procedimentos reforçados de segurança e proteção de dados, incluindo restrição de acesso, pseudonimização, criptografia e outras medidas técnicas de proteção de informações, assim como sejam tomadas precauções para evitar o compartilhamento de dados sensíveis para terceiros não autorizados.

IV. **Os tratamentos de dados pessoais sensíveis serão, de acordo com sua natureza e escala, precedidos de análise de risco, sendo recomendável que se proceda, em caso de risco relevante, à realização de um Relatório de Impacto à Proteção de Dados, documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares de dados, juntamente com quais medidas foram adotadas para a mitigação destes riscos.**

2.7.3. MONITORAMENTO DE SAÚDE EM PERÍODOS DE EMERGÊNCIA SANITÁRIA

Algumas modalidades de tratamento de dados pessoais com o objetivo de combate à pandemia do Covid-19 revelaram a necessidade de proporcionar segurança para empresas e sociedade na utilização de dados pessoais para fins de natureza humanitários e no interesse público, por meio das ações contra a emergência epidemiológica.

Neste sentido, há que se considerar a finalidade última da LGPD - a proteção da pessoa, evidenciada nas hipóteses de utilização de dados pessoais para proteção da vida, incolumidade física e saúde. É possível concluir que o tratamento de dados pessoais para fins de combate à pandemia é legítimo e pode mesmo se afigurar como um imperativo relacionado ao interesse público, sempre que realizados com os devidos cuidados e ressalvas para que não resultem em prejuízo para os titulares e tampouco para as empresas ou organizações, através da aplicação de princípios como os da necessidade, prevenção e segurança, entre outros.

I. **Os tratamentos de dados pessoais de passageiros, terceirizados e trabalhadores em geral, realizados para fins de combate à Covid-19 ou, de forma geral, outros tipos de pandemia ou doenças endêmicas, devem ser realizados estritamente com este objetivo, não podendo ser aproveitados para finalidades de outra natureza sem que haja autorização expressa do titular ou previsão legal específica, o que pode significar que prazos de retenção de dados pessoais, de acordo com as políticas das organizações, sejam mais restritos.**

II. **As medidas de controle de acesso que utilizem ou revelem dados sensíveis de saúde que eventualmente impliquem em restrições ao transporte de passageiros serão implementadas de forma a restringir, na medida do possível, o acesso ou conhecimento das informações pessoais envolvidas por terceiros. Os referidos dados de saúde, além das restrições citadas no tópico sobre dados sensíveis, terão controle restrito de acesso - de preferência apenas acessíveis por profissionais de saúde – e somente serão comunicados ao próprio passageiro, ou no caso de obrigação legal ou regulatória que obrigue o compartilhamento dessas informações.**

2.7.4. TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Os dados pessoais de crianças e adolescentes merecem proteção especial, de acordo com o estágio de desenvolvimento cognitivo, social e intelectual desta categoria de titulares, levando-se em conta o seu melhor interesse e considerando necessariamente a autorização dos pais ou responsáveis legais no caso de crianças, compreendidas como aquelas que possuem até 12 (doze) anos de idade incompletos. O acesso de crianças e adolescentes aos serviços de transporte levará este regime em conta.

I. **Dados pessoais de crianças somente serão tratados na medida em que houver estrita necessidade para a prestação do serviço de transporte ou exigência legal. Os dados pessoais dos pais ou representantes legais, que fornecerão os dados da criança e devem autorizar o seu tratamento, serão igualmente tratados. Exige-se, neste caso, o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo seu responsável legal, cujos dados também serão tratados para o fim estrito da prestação do serviço de transporte ou exigência legal.**

II. **Toda documentação necessária por exigência legal ou regulatória para a prestação do serviço de transporte de crianças e adolescentes que inclua seus dados pessoais será utilizada unicamente para este fim e disponibilizada às autoridades quando necessário, devendo lhe ser conferida proteção especial e compartilhada somente em situações decorrentes de exigência legal ou regulatória.**

2.7.5. OUVIDORIA, SAC E CANAL DE COMUNICAÇÃO COM ENCARREGADO

I. As empresas ou entidades estabelecerão canais de comunicação que possibilitem aos passageiros e demais titulares de dados obter informações e exercer seus direitos em relação aos seus dados pessoais. Este canal pode ser exclusivo para questões referentes aos dados pessoais ou, conforme a conveniência, volume e demais aspectos relevantes, integrar a estrutura de outros canais de comunicação, como o Serviço de Atendimento ao Consumidor (SAC), Ouvidoria ou outros.

II. Considerando ser a proteção de dados tema recentemente introduzido na legislação brasileira, recomenda-se que os atendentes que representam a organização frente ao titular sejam devidamente treinados em relação ao cumprimento dos direitos dos titulares, buscando a melhoria dos serviços aos titulares, a proteção de seus direitos e evitando o dano reputacional à empresa ou organização.

III. Será dada ampla publicidade ao canal de comunicação oferecido para informações e resolução de questões referentes ao tratamento de dados pessoais, sendo indicadas as formas de acesso a este canal de forma ampla aos passageiros e demais titulares.

IV. Será dada ampla publicidade ao contato do encarregado de proteção de dados.

V. O encarregado de proteção de dados deverá zelar para que as demandas de passageiros e titulares de dados que sejam dirigidas aos canais de comunicação, bem como as que lhe chegarem diretamente, sejam devidamente encaminhadas aos setores responsáveis para que sejam atendidas em tempo hábil e em cumprimento às regras legais aplicáveis.

VI. **Independentemente do meio pelo qual o titular entrar em contato com a organização, a empresa ou organização deverá ser transparente em relação ao uso dos seus dados, incluindo elementos como avisos de privacidade ou demais documentos relevantes. Caso seja necessário o consentimento ou anuência do titular que entra em contato via telefone ou aplicativo de mensageria, é possível a utilização de árvores de decisão a serem disponibilizadas ao titular para se expressar, seja por voz, texto ou teclando número em menu digital, podendo tais declarações serem armazenadas para fins de comprovação.**

2.7.6. COMPARTILHAMENTO DE DADOS COM TERCEIROS

A prestação de serviços de transportes de passageiros e de carga pode demandar o compartilhamento de dados pessoais com parceiros e empresas terceiras à relação, a exemplo de prestadores de serviços, agências de viagens, empresas de assistências de passageiros, entre outros. Este compartilhamento pode se dar por imposição legal ou regulatória, ou para outras finalidades.

I. **Além da necessária transparência acerca destas atividades de tratamento aos titulares de dados pessoais, é importante que os contratos celebrados com terceiros contenham disposições aplicáveis em matéria de privacidade e proteção de dados capazes de garantir a proteção de dados para além dos ambientes de cada empresa ou organização.**

II. **Os contratos com terceiros que incluam o compartilhamento de dados pessoais devem incluir disposições sobre medidas necessárias para a segurança das informações compartilhadas, as finalidades estritas do tratamento de dados, as responsabilidades das partes em responder a questionamentos das autoridades e dos titulares e obrigação de reportar eventuais incidentes de dados em tempo hábil, entre outros pontos necessários à preservação dos direitos e garantias dos titulares que a lei imponha.**

2.8. PROTOCOLO DE EMPREGADOS E PRESTADORES DE SERVIÇO

Os empregados de uma empresa ou organização representam uma das categorias de titulares de dados de maior relevância, especialmente diante da natureza sensível de parte dos dados pessoais que habitualmente são coletados e tratados durante a relação trabalhista.

Em razão do desequilíbrio conjuntural de poder nas relações de trabalho, resulta a dificuldade e mesmo improbabilidade de que o empregado forneça consentimento para o tratamento de seus dados pessoais que possa ser considerado, efetivamente, livre. Contudo, podem haver situações em que seja possível ao empregado dar o seu consentimento de forma livre em circunstâncias excepcionais, ou seja, quando o ato de dar ou recusar o consentimento não produza consequências negativas para ele, casos nos quais deve-se preocupar em propiciar os elementos necessários para que tal liberdade seja efetiva, bem como possibilitar a sua demonstração.

Desde a fase pré-contratual, até após a rescisão do contrato de trabalho, o empregador poderá assumir o papel de controlador dos dados pessoais de seus empregados, possuindo poder decisório sobre o tratamento dos dados pessoais coletados dos empregados, a exemplo de sua documentação pessoal de identificação, imagens no ambiente de trabalho, em chamadas de sistemas de videoconferência das quais participa, o registro biométrico da jornada de trabalho, entre outros.

Eventualmente a empresa ou organização poderá terceirizar atividades que envolvam o tratamento de dados de seus empregados, a exemplo de contratações de empresas responsáveis por gestão de folha de pagamento ou mesmo procedimentos de recursos humanos, situações em que deverá garantir que as regras aplicáveis à privacidade e proteção de dados pessoais sejam também observadas por todos os envolvidos no tratamento de dados de seus empregados.

Nesse sentido, mostra-se extremamente importante adotar medidas práticas que considerem as especificidades desta relação, considerando especialmente o incremento do trabalho home office ou teletrabalho durante o período pandêmico, que exige atenção redobrada sobre o assunto.

2.8.1. PROCESSO SELETIVO

Durante processos seletivos e de recrutamento é fundamental que sejam coletados apenas os dados estritamente necessários para realizar a seleção, ou seja, solicitar a menor quantidade possível de dados pessoais, tendo cautela inclusive quanto a pedidos de informações pretéritas do candidato. Nos casos em que forem utilizadas ferramentas automatizadas para filtrar currículos, as empresas e organizações devem evidenciar os critérios e procedimentos utilizados para a decisão automatizada e pautar-se pelo princípio da não discriminação, a fim de que não sejam coletados dados sensíveis que possam causar discriminação entre os candidatos.

Além disso, recomenda-se que, para o armazenamento dos currículos dos candidatos não selecionados, seja preferencialmente obtido o consentimento destes por meio de instrumento ou manifestação específica, destacando o período em que tal documento ficará retido pela empresa ou organização, sendo que para a coleta e o armazenamento de dados sensíveis – como, por exemplo, dados sobre deficiências - seja necessário recorrer ao consentimento como base legal.

Caso o candidato se oponha ao tratamento, as empresas e organizações devem obrigatoriamente descartar os dados pessoais obtidos mediante consentimento de forma segura, gerando, sempre que possível, evidências que comprovem a eliminação dos dados pelo recurso de procedimentos técnicos que o atestem. Para dados pessoais que não tenham sido obtidos via consentimento, a empresa ou organização poderá manter os dados pessoais, contanto que persista finalidade específica e base legal que o autorize. Ainda, recomenda-se que eventuais anotações registradas durante entrevista de seleção e recrutamento sejam devidamente descartadas logo depois de encerrado o processo.

2.8.2. CONTRATO DE TRABALHO: ADMISSÃO, EXECUÇÃO E ENCERRAMENTO

Para formalização do contrato de trabalho pode ser necessário coletar uma variedade de dados pessoais e dados pessoais sensíveis do empregado. As empresas e organizações devem providenciar todos os cuidados necessários para que não sejam coletados dados pessoais em excesso e para que o titular, ao fornecer os dados necessários, tenha pleno conhecimento da finalidade para a qual cada um deles foi coletado, inclusive a respeito dos possíveis compartilhamentos que podem ser feitos diante de obrigações legais ou regulatórias. Nesse sentido, é ainda mais importante que as empresas e organizações informem ao empregado a sua política de tratamento de dados, solicitando a ele, sempre que possível, a assinatura de termo de ciência quanto ao seu conteúdo.

Além disso, a manutenção do contrato de trabalho exige atualizações periódicas dos dados pessoais constantes da ficha do empregado que contém o seu histórico dentro da empresa ou organização, incluindo atestados médicos, licenças e processos disciplinares internos. Dessa forma, considerando a sensibilidade e confidencialidade dos dados pessoais que compõem a ficha do empregado, é fundamental que o acesso lógico ou físico a tais documentos seja restrito apenas a pessoas expressamente autorizadas.

Quanto ao encerramento do contrato de trabalho, recomenda-se que as empresas e organizações atentem-se aos prazos legais e regulatórios de guarda e retenção dos dados pessoais dos empregados, observando a finalidade e base legal para o armazenamento de dados pessoais como, por exemplo, para exercício de direito em processos judiciais e arbitrais pela organização. Após o decurso do prazo de guarda ou retenção destas informações, as empresas ou organizações devem promover o seu efetivo descarte. Recomenda-se, nestes casos, a manutenção de um inventário de dados pessoais tratados pela empresa ou organização, documento que poderá facilitar a gestão dos dados pessoais, inclusive o controle dos períodos de retenção destas informações.

2.8.3. TRATAMENTO DE DADOS SENSÍVEIS

Em relação ao tratamento de dados pessoais sensíveis, elencados pela Lei como aqueles de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, é fundamental considerar que sua definição é dinâmica, já que, a partir de dados pessoais que não sejam sensíveis é também possível se chegar a informações sensíveis. Por exemplo, o nome do cônjuge pode revelar a opção sexual do titular, o seu nome e a forma como se veste em uma foto pode revelar sua orientação religiosa, assim como o seu sobrenome ou outros dados podem revelar sua origem étnica.

As empresas e organizações devem assim avaliar a natureza dos dados sempre caso a caso, justamente para que seja possível definir a melhor base legal aplicável. Isso porque, no caso de dados pessoais sensíveis, exclui-se a possibilidade de tratamento mediante bases legais, como as de execução de contratos, de legítimo interesse do controlador e de proteção do crédito. Por outro lado, é possível tratá-los para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, bem como para cumprimento de obrigação legal ou regulatória pelo controlador e exercício regular de direitos, em contrato e em processo judicial, administrativo e arbitral, fundamentos mais comuns no tratamento de dados pessoais de empregados.

Nos casos em que dados sensíveis forem coletados no processo de contratação para fins de promoção de diversidade, inclusão e implementação de políticas de ação afirmativa, estas finalidades, bem como os critérios de seleção, serão divulgadas e o fornecimento das referidas informações será realizado mediante consentimento específico.

2.8.4. MONITORAMENTO DE SAÚDE EM PERÍODOS DE EMERGÊNCIA SANITÁRIA

Considerando a necessidade de monitoramento da saúde dos empregados em períodos pandêmicos, as empresas e organizações devem realizar o tratamento de dados na medida do que seja estritamente necessário para o alcance deste fim, utilizando somente dados que sejam pertinentes, proporcionais e não excessivos em relação à esta finalidade. Nesse sentido, recomenda-se que seja sempre realizada uma ponderação entre a tutela da saúde da população e a proteção da privacidade dos titulares. Assim, a segurança no tratamento dos dados assume ainda maior relevância, bem como a transparência no tratamento e a prévia definição e divulgação dos procedimentos de retenção, compartilhamento e eliminação, considerando especialmente o cenário de vulnerabilidade informacional e fática decorrente até mesmo de fatores de saúde. Há, ainda, que se considerar que a LGPD proíbe a comunicação e o uso compartilhado de dados sensíveis referentes à saúde entre controladores quando houver objetivo de obter vantagem econômica, salvo para a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

2.8.5. COMPARTILHAMENTO DE DADOS COM TERCEIROS

As empresas e organizações devem informar ao empregado, no ato da contratação, sobre possíveis compartilhamentos que serão realizados com seus dados pessoais para manutenção de contratos de benefícios, tais como vale-transporte, vale-refeição, vale-alimentação, plano de saúde e/ou odontológico, cestas, convênios, bolsas de estudo, descontos, entre outros, advindos ou não de acordos coletivos, convenções coletivas ou mesmo disponibilizados por mera liberalidade de cada empresa e organização.

As eventuais limitações ou impossibilidades relacionadas à opção do empregado em não compartilhar seus dados para estas finalidades deverão ser igualmente informadas. Somente deverão ser compartilhados os dados estritamente necessários para a concessão do benefício e as empresas e organizações devem

zelar pelo tratamento escorreito desses dados pelos operadores, a fim de que seja realizado dentro das expectativas legítimas dos titulares e dos limites impostos pela LGPD. Recomenda-se também que as empresas e organizações realizem auditorias periódicas nos sistemas e nas medidas técnicas e organizacionais das empresas administradoras dos benefícios, a fim de garantir a licitude do tratamento dos dados, e revisem os contratos firmados com elas, incluindo cláusulas de proteção de dados, confidencialidade, dentre outras que se façam necessárias.

2.8.6. CONTRATAÇÃO DE PRESTADORES DE SERVIÇO

Quando, por ocasião da contratação de prestadores de serviço, for necessário o tratamento de seus dados pessoais ou de seus representantes legais, as empresas e organizações devem evitar, neste procedimento, a coleta de dados pessoais em excesso e, ainda, zelar para que o titular, ao fornecer os dados necessários, tenha pleno conhecimento da finalidade para a qual foram coletados, inclusive a respeito dos possíveis compartilhamentos que podem ser feitos diante de obrigações legais ou regulatórias. Ainda, caso haja atualização periódica de dados dos empregados dos prestadores de serviço, recomenda-se que o acesso lógico ou físico a tais documentos seja restrito apenas a agentes expressamente autorizados.

Quanto ao encerramento do contrato de prestação de serviço, recomenda-se que as empresas e organizações atentem-se aos prazos legais e regulatórios que porventura sejam aplicáveis para a guarda e retenção dos dados pessoais dos empregados dos seus prestadores de serviço e, quanto aos dados que não são mais necessários para tais finalidades, realizem o seu descarte consciente e cuidadoso.

2.8.7. SAÚDE E SEGURANÇA DO TRABALHO

Os dados pessoais referentes à saúde e à segurança do trabalho devem ser tratados por empresas e organizações para finalidades estritamente determinadas, de forma proporcional e pautadas no princípio da não discriminação. Tais dados podem incluir, entre outras, informações relacionadas ao estado de saúde dos indivíduos, como

Protocolos Gerais

lesões, doenças, incapacidade ou risco de doença, histórico médico, pareceres, diagnósticos e tratamento clínico, exames médicos, resultados de testes, dados de dispositivos médicos ou dados de rastreadores de aptidão, além dos dados obtidos pelas operadoras de saúde ou referentes ao tratamento contínuo de enfermidades, detalhes de consulta, faturas e outros que revelem aspectos da saúde do titular.

I. **Quanto à realização de exames periódicos, estes devem se limitar aos casos em que sejam relevantes para o desempenho de funções específicas pelo empregado, excluindo-se aqueles nos quais não há esta relação. Assim, por exemplo, não se justifica a realização do exame toxicológico para empregados do setor administrativo ou o exame de gravidez por ocasião da admissão. O resultado e demais dados atinentes aos exames não podem ser revelados para além do titular e das pessoas justificadamente autorizadas dentro de uma estrutura organizacional.**

II. **Em relação ao recebimento de atestados médicos referentes a funcionários em uma determinada organização, por se tratarem de informações sensíveis, recomenda-se à instituição uma política de tratamento, retenção e acesso específica. Recomenda-se ainda que as empresas e organizações armazenem esses dados em ambiente separado com controle de acesso que somente autorize o ingresso de pessoas autorizadas.**

III. **Durante a eventual realização de pesquisas internas para aferir a produtividade e bem-estar físico e mental dos empregados, é fundamental que sua privacidade seja resguardada. Nesses casos, recomenda-se a utilização de técnicas de anonimização ou pseudonimização para o tratamento dos referidos dados, de forma a resguardar a identidade do titular e, ao mesmo tempo, alcançar os resultados almejados.**

Protocolos Gerais

IV. **Em períodos pandêmicos há demandas específicas relacionadas a protocolos de saúde e segurança do trabalho, considerando especialmente as exigências de autoridades administrativas e judiciais. Nesse sentido, pode ser necessário o tratamento de uma quantidade adicional de dados pessoais e, especialmente, dados pessoais sensíveis por diversos motivos, como verificar quais funções devem retornar primeiro ao trabalho, quais são os grupos de risco, quais as atividades com maior risco de exposição, determinação de regras de teletrabalho/home office, meios de locomoção, alternativas de rodízio de trabalho ou atividades, testagem recorrente ou sintomas de alertas, controle de entrada e saída presencial, período de troca de máscara, uso do álcool gel e a higienização dos ambientes de trabalho, entre outros. Nesse aspecto, as empresas e organizações devem conferir especial atenção ao tratamento desses dados, resguardando a segurança do titular e a transparência sobre os procedimentos adotados a respeito de quais dados estão sendo coletados, para quais finalidades, por quanto tempo ficarão retidos, quais são seus direitos enquanto titular de dados, entre outras informações. Além disso, as empresas e organizações devem se comprometer a não tratar tais dados para finalidades diversas daquelas informadas e a não compartilhar os dados sem a prévia comunicação do titular e, quando necessário, o seu consentimento.**

V. **Com relação à realização de exames admissionais, fiscalização e controle de jornada de trabalho (por meio do registro de ponto, por exemplo) e atividades ligadas à segurança do trabalho (como a realização de testes toxicológicos, do uso do etilômetro e outros exames médicos), as empresas e organizações devem atentar às diretrizes legais e regulatórias sobre a necessidade da coleta de tais dados e as finalidades formalmente instituídas para o seu tratamento. Por se tratar, na maioria das vezes, do cumprimento de obrigações legais ou regulatórias, o tratamento deve estar restrito ao mínimo necessário para adimplir com tais obrigações, evitando-se a coleta e tratamento de dados pessoais desnecessários ou excessivos, bem como a sua utilização para além do cumprimento da referida obrigação.**

Protocolos Gerais

VI. **No tratamento de dados relacionados à gestão de saúde e segurança do trabalho em uma empresa ou organização, é comum a contratação de parceiros, como clínicas médicas, prestadores de serviço da área de engenharia do trabalho ou mesmo a contratação de sistemas informatizados de gestão de pessoal, como procedimentos de recursos humanos ou controle de ponto. Assim, nos casos em que ocorra o tratamento de informações sensíveis por terceiros, faz-se necessária análise criteriosa sobre o nível de adequação destes parceiros à LGPD, bem como a necessidade de adequação contratual para que sejam dispostos claramente quais os direitos e obrigações de cada parte envolvida na relação firmada, principalmente em matérias relacionadas a medidas técnicas e administrativas de segurança da informação e protocolos para gestão de incidentes de informação.**

VII. **Especificamente quanto ao compartilhamento de dados pessoais para o oferecimento de planos de saúde e/ou odontológicos corporativos, é fundamental que as empresas e organizações atentem a situações específicas, como no caso de tratamento de dados pessoais de dependentes, particularmente menores de idade ou idosos. Vale ressaltar que a LGPD dispõe de regras específicas para o tratamento de dados pessoais de crianças e adolescentes, que sempre deverá resguardar o seu melhor interesse.**

>> CAPÍTULO 3

Protocolos Específicos

3.1. PROTOCOLO DE CARTÕES DE TRANSPORTE

Os sistemas de bilhetagem eletrônica realizam tratamento de dados pessoais e, em alguns casos, de dados pessoais sensíveis, mais especificamente dados biométricos, além de dados pessoais de crianças, adolescentes e idosos. Em determinados arranjos podem também permitir a compilação de hábitos referentes ao deslocamento de seus usuários. Como diversas atividades necessárias à operacionalização desses sistemas se utilizam de dados pessoais, é imperativa a sua compatibilidade com os parâmetros da LGPD.

Um sistema de bilhetagem eletrônica funciona, em linhas gerais, como uma espécie de cartão pré-pago, no qual o usuário insere no cartão um determinado valor, que será descontado à medida que o saldo é utilizado para a utilização de serviços de transportes. Um exemplo de bilhetagem eletrônica é o Bilhete Único, um modelo baseado em cartão que armazena valores para o pagamento de passagens no transporte público em uma determinada rede de transporte (ônibus, micro-ônibus, Metrô ou trem urbano).

Diante disso, tanto no ato de emissão do cartão quanto, eventualmente, no ato de recarga e na sua própria utilização, são coletados dados pessoais. Os dados pessoais tratados podem variar, a depender da empresa, da regulamentação específica do local onde o serviço é prestado ou do próprio sistema de bilhetagem. Assim, a implementação de um sistema de cartão de transporte pode assumir diversas feições.

O sistema de bilhetagem eletrônica também deve considerar políticas de descontos ou isenção de preço (gratuidade), o que pode, eventualmente, implicar na necessidade de tratamento de dados pessoais para a autenticação de usuários beneficiados por esta política. Para a autenticação de usuários eventualmente são utilizados dados biométricos como recurso para combater possíveis fraudes.

Protocolos Específicos

3.1.1 OPERAÇÕES DE TRATAMENTO DE DADOS EM CARTÕES DE TRANSPORTE

As principais atividades de tratamento de dados pessoais comumente realizadas pelas empresas e organizações do setor de transporte quanto aos cartões de transporte encontram-se relacionadas abaixo, com destaque às principais características do tratamento, que devem ser observadas.

3.1.2. TRATAMENTO DE DADOS PESSOAIS DE USUÁRIOS DOS SERVIÇOS DE TRANSPORTE PARA EMISSÃO E RECARGA DE CARTÕES DE TRANSPORTE

TITULAR DOS DADOS	São os usuários dos serviços de transporte. Nos casos de determinadas categorias de pessoas contempladas com benefícios tarifários, o titular de dados poderá ser criança ou adolescente. Nessa hipótese, é indispensável a observância do art. 14 da LGPD, especialmente no que se refere à realização do tratamento de dados pessoais no seu melhor interesse, observando-se, entre outros, a necessidade de transparência, bem como a observância das regras legais acerca do consentimento ou assistência de pais ou responsáveis para o tratamento de dados pessoais. Para os usuários idosos, há casos nos quais são cadastrados e possuem cartão de transporte específico. Nessas situações costumam ser solicitadas algumas informações para fins de elegibilidade a benefícios e autenticação. No caso de pessoas com necessidades especiais, a realização do seu cadastramento, além dos dados básicos de identificação, contempla também a coleta de dados sensíveis, que devem ser tratados com procedimentos específicos. Nos casos de outras gratuidades, a depender das especificades definidas legalmente para cada sistema de transporte, outras categorias de usuários do sistema de transporte podem ser titulares dos dados.

Protocolos Específicos

FINALIDADE DO TRATAMENTO	Emissão e recarga do cartão de transporte (tanto cartões de gratuidade quanto cartões de comercialização) para utilização pelo usuário do serviço.
AGENTES DE TRATAMENTO	A depender do caso concreto, as Prestadoras de Serviços de Transporte podem ser controladores ou operadores dos dados pessoais. Isso porque, em alguns casos, o controle é realizado pelo próprio Governo ou Município e as Prestadoras de Serviços de Transporte realizam o tratamento justamente para operacionalizar e viabilizar o uso da bilhetagem eletrônica, como ocorre no caso dos contemplados com benefícios tarifários específicos.
PERÍODO DE ARMAZENAMENTO DOS DADOS	Operíododearmazenamentodeveseguiroprincípiodaminimização. Os dados biométricos, quando tratados, devem ser mantidos pelo tempo que forem pertinentes, limitados aos fins para os quais são tratados. Ainda que a LGPD não estabeleça um prazo limite para armazenamento de dados biométricos, recomenda-se que tão logo eles não sejam mais necessários, devam ser prontamente eliminados.

3.1.3. TRATAMENTO DE DADOS PESSOAIS DE COLABORADORES CELETISTAS PARA CONCESSÃO DO BENEFÍCIO DE VALE-TRANSPORTE

TITULAR DOS DADOS	Colaboradores das prestadoras de serviços de transporte
FINALIDADE DO TRATAMENTO	Concessão mensal do benefício de vale-transporte ao colaborador celetista.
BASES LEGAIS QUE EVENTUALMENTE PODEM SER UTILIZADAS	Nos casos de benefício sem uso de dados pessoais sensíveis: Art. 7º, VI, IX, da LGPD. Nos casos de gratuidade: Art. 11, II, "a", da LGPD. Cumprimento de obrigação legal ou regulatória pelo controlador. O vale-transporte é regulamentado pela Lei nº. 7.418/85. Sua concessão é obrigatória para todos os trabalhadores brasileiros, que façam parte do quadro de colaboradores de uma empresa.
PERÍODO DE ARMAZENAMENTO DOS DADOS	Operíododearmazenamentodeveseguiroprincípiodaminimização. Os dados biométricos, quando tratados, devem ser mantidos pelo tempo que forem pertinentes, adequados e limitados aos fins para os quais são tratados. Ainda que a LGPD não estabeleça um prazo limite para armazenamento de dados biométricos, recomenda-se que tão logo eles não sejam mais necessários devam ser prontamente eliminados.

3.1.4. BOAS PRÁTICAS NO TRATAMENTO DE DADOS EM CARTÕES DE TRANSPORTE

I. O termo de adesão do usuário de cartões de transporte deve especificar, de forma clara, as informações relacionadas ao tratamento dos seus dados pessoais, conforme determina o art. 9º da LGPD, especialmente quanto às categorias de dados coletados, o tempo de duração do tratamento, o prazo de retenção dos dados, a base legal que fundamenta o tratamento, a finalidade, entre outras informações que sejam essenciais para a devida transparência no tratamento dos dados.

II. As empresas prestadoras de serviços de transporte devem proporcionar as devidas garantias aos dados pessoais dos usuários de cartões de transporte quando estas forem responsáveis pelas recargas de vale-transporte dos seus colaboradores. Nos casos em que houver a contratação de empresas para fornecimento de vale-transporte, o compartilhamento de dados pessoais deve se restringir àqueles estritamente necessários, pertinentes e adequados para a concessão dos benefícios.

III. As empresas prestadoras de serviço de transporte não devem utilizar informações referentes aos deslocamentos para finalidades que não estejam relacionadas diretamente ao funcionamento e melhoramento do sistema de transportes sem o consentimento dos passageiros, o que não poderá ser condição para a utilização do serviço de transporte. Da mesma forma, esses dados não devem ser disponibilizados para terceiros para fins econômicos não relacionados à prestação do serviço de transporte, salvo se obtido o referido consentimento.

IV. A utilização de dados pessoais de localização dos usuários dos serviços de transporte para controle geográfico (de tráfego) e para fins estatísticos deve ser previamente comunicada ao titular dos dados, constando também da Política de Privacidade ou outros documentos equivalentes. As empresas e organizações

procederão, preferencialmente, à anonimização ou, quando esta não for possível, a pseudonimização desses dados para sua utilização para fins estatísticos.

V. As empresas e organizações deverão, preferencialmente, oferecer aos usuários a possibilidade de eliminação ou anonimização de seus dados pessoais, particularmente aqueles referentes às compras e recargas ou a efetiva utilização de cartões de transporte que permitam que seus deslocamentos sejam conhecidos. Nos casos em que houver necessidade de manutenção de dados para a operação do serviço com base no art. 15, I, da LGPD e, à luz do art. 16, I, da LGPD, a respectiva justificativa deve ser comunicada aos titulares por meio de políticas de privacidade ou documentos equivalentes.

VI. As empresas e organizações devem garantir que todos os fornecedores com acesso às bases de dados para implantação do sistema de bilhetagem eletrônica estejam em conformidade com a LGPD. Além disso, devem lhes fornecer instruções claras sobre como proceder com o tratamento dos dados pessoais para a finalidade acordada, assegurando-se que os dados não serão utilizados para outras finalidades e nem mesmo compartilhados com terceiros sem sua autorização.

VII. Quando a recarga do cartão de transporte estiver condicionada ao fornecimento de dados pessoais adicionais em relação àqueles já coletados no momento de emissão do cartão, o titular deverá ser informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados na LGPD.

VIII. A depender dos regulamentos e políticas públicas que sejam aplicáveis, o sistema de bilhetagem eletrônica pode prever políticas de descontos ou isenção de preço (gratuidade), o que pode, eventualmente, tornar necessário o tratamento de dados pessoais de titulares específicos, a exemplo de pessoas contempladas com benefícios tarifários, ou mesmo ensejar a demanda por tratamento de dados pessoais

Protocolos Específicos

adicionais para fins de prevenção de fraude na utilização do benefício. Nesses casos, é fundamental observar o regramento especial da LGPD para determinadas categorias de titulares e para a categoria de dados pessoais sensíveis, conforme seja aplicável. A utilização desses dados, de todo modo, deverá seguir estritamente o princípio da minimização e a circunscrição do tratamento à sua finalidade, bem como a transparência sobre o tratamento e seus aspectos principais.

3.2. PROTOCOLO DE DADOS BIOMÉTRICOS, IMAGEM E RECONHECIMENTO FACIAL

No setor de transporte, o recurso a dados biométricos para validação biométrica de identidade vem sendo utilizado com certa frequência, buscando eficiência e efetividade operacional em políticas de controle de acesso, prevenção de fraudes e segurança. O exemplo a seguir ilustra um caso de recurso a dados biométricos:

O prédio de uma prestadora de serviços de transporte apresenta um sistema eletrônico de digitalização de impressões digitais. Os seguranças fazem a varredura das impressões digitais dos colaboradores para que eles possam passar pelas catracas de entrada a uma área restrita do prédio.

Este sistema está processando dados biométricos para identificar colaboradores individualmente, a fim de confirmar se eles possuem autorização de acesso à área restrita. Diante disso, a prestadora de serviços de transporte precisará observar as disposições da LGPD para tratar esses dados.

>> CAPÍTULO 3

Protocolos Específicos

A utilização de dados biométricos implica na tomada de precauções para que sua utilização seja legítima. A depender da forma como forem tratados, os dados biométricos podem conferir aos controladores uma capacidade considerável de monitoramento das atividades dos titulares, abrindo margem à ameaça ou violações aos direitos e garantias fundamentais dos titulares. Exatamente por isso a utilização de dados biométricos no setor de transporte merece atenção especial e deve ser realizada de forma proporcional, adequada, transparente e em conformidade com a LGPD.

Quanto à sua natureza, os dados biométricos são expressamente identificados no art. 5º, inc. II, da LGPD[1] como dados pessoais sensíveis – o que implica na necessidade de que seu tratamento esteja amparado em uma das bases legais dispostas no art. 11.

Para termos um parâmetro, o Regulamento Europeu de Proteção de Dados (RGPD) define dados biométricos como dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa, como imagens faciais ou as impressões digitais.

No entanto, apesar de a LGPD não disciplinar um conceito expresso para os dados biométricos, é possível constatar que a biometria não se restringe à impressão digital (seja a palma da mão, sejam as digitais dos dedos) e às imagens faciais (como o formato da face), mas pode ser também extraída a partir da retina ou íris dos olhos, da voz, do DNA, do padrão das veias e até mesmo da deambulação – que representa a forma como determinada pessoa caminha, ou seja, sua maneira de andar[2]. O quadro

1. Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

2. Destaca-se, nesse sentido, o conceito de atributos biométricos apresentado no inc. II do art. 2º do Decreto 10.046/2019, qual seja "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar". Além disso, é importante conferir também o conceito de informação biométrica previsto no California Consumer Privacy Act (CCPA), título 1.81.5, 1798.140, (b), qual seja "características fisiológicas, biológicas ou comportamentais de um indivíduo, incluindo informações relativas ao ácido desoxir-ribonucleico (DNA) de um indivíduo, que é usado ou destinado a ser usado, individualmente ou em combinação uns com os outros ou com outros dados de identificação, para estabelecer identidade individual. As informações biométricas incluem, mas não estão limitadas a imagens da íris, retina, impressão digital, rosto, mão, palma, padrões de veias e gravações de voz, a partir das quais um modelo de identificador, como uma impressão facial, um modelo de minúcias ou uma impressão de voz, podem ser extraídos e padrões ou ritmos de pressionamento de tecla, padrões ou ritmos de marcha e dados de sono, saúde ou exercícios que contêm informações de identificação".

Protocolos Específicos

abaixo sintetiza, nesse sentido, exemplos de técnicas de identificação biométrica física ou fisiológica e comportamental.

TÉCNICAS DE IDENTIFICAÇÃO BIOMÉTRICA FÍSICA OU FISIOLÓGICA	• Reconhecimento facial; • Verificação de impressão digital; • Varredura da íris; • Análise da retina; • Reconhecimento de voz; e • Reconhecimento de formato de orelha.
TÉCNICAS DE IDENTIFICAÇÃO BIOMÉTRICA COMPORTAMENTAL	• Análise de pressionamento de tecla; • Análise de assinaturas manuscritas; • Análise de marcha; e • Análise do olhar (rastreamento ocular).

Assim, é possível constatar que uma das características principais dos dados biométricos é o fato de que eles possuem, em muitos casos, uma ligação única com indivíduos específicos, o que aumenta bastante o seu potencial de identificabilidade em termos de precisão. Ou seja, trata-se de um dado que, na maior parte das vezes, não apenas torna uma pessoa natural identificável, mas a identifica diretamente, independentemente de cruzamentos com outros tipos de dados, além de, diferentemente de sistemas que se utilizam de identificadores externos (como um número de identidade), os dados biométricos são reflexo de características físicas, geralmente inatas, da pessoa e não podem ser substituídas - o que implica na necessidade de que sejam tratados com cautela extrema.

Protocolos Específicos

Por exemplo, será sempre possível alterar a senha de um cartão de crédito em caso de fraude, mas não é possível modificar a íris ou impressão digital de uma pessoa. No entanto, é importante destacar que até mesmo características biométricas não são únicas, como o modo de andar de um indivíduo, ainda assim podem servir para excluir uma série de outras pessoas de um processo de classificação e, em conjunto com outros dados, levar à sua identificação.

Verifique-se, ainda, que a consideração do dado como biométrico por vezes pode levar em conta aspectos do contexto do seu tratamento, e não somente dos dados pessoais em si. O Conselho Europeu de Proteção de Dados (European Data Protection Board - EDPB) já entendeu que imagens de vídeo de uma pessoa não são consideradas, em si, dados biométricos, uma vez que o processamento técnico dessas imagens não foi originalmente pensado para produzir a identificação do indivíduo. Assim, a definição prática do dado biométrico pressupõe ainda um processamento técnico específico e a intenção do controlador em permitir a identificação de uma pessoa natural específica[1].

Essa, inclusive, é propriamente a previsão do Considerando 51 do Regulamento Geral de Proteção de Dados da União Europeia, que esclarece que o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados (conceitualmente similar à categoria de dados sensíveis na LGPD), uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa natural.

1. Tal entendimento pode ser encontrado nas Guidelines 3/2019 on processing of personal data through video devices, de 10 de julho de 2019. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

Protocolos Específicos

3.2.1. OPERAÇÕES DE TRATAMENTO DE DADOS BIOMÉTRICOS

As atividades de tratamento de dados biométricos comumente realizadas pelas empresas e organizações do setor de transporte encontram-se relacionadas abaixo, individualmente, com destaque às principais características do tratamento, que devem ser observadas por todos os destinatários do presente Guia de Boas Práticas.

3.2.2. TRATAMENTO DE DADOS BIOMÉTRICOS DE USUÁRIOS DOS SERVIÇOS DE TRANSPORTE PARA GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR NO USO DE CARTÕES DE TRANSPORTE

TITULAR DOS DADOS	Categorias especiais de usuários de transporte. Destaca-se que, nos casos de passe estudantil, o titular de dados será menor de idade, ou seja, criança ou adolescente. Nessa hipótese, é indispensável a observância do art. 14 da LGPD, especialmente no que se refere à realização do tratamento no seu melhor interesse.
FINALIDADE DO TRATAMENTO	Identificar usuários e impedir fraudes no uso de cartões de transporte. Ou seja, coibir o uso indevido por pessoas que não são titulares do cartão ou que não fazem jus ao benefício das modalidades específicas da bilhetagem eletrônica (estudante, idoso, passe livre para estudantes de escolas públicas, etc.).
POSSÍVEL BASE LEGAL	Art. 11, II, "g", da LGPD. Garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Protocolos Específicos

AGENTES DE TRATAMENTO	Controlador: Prestadoras de Serviços de Transporte ou Poder Concedente. Operador: Prestadoras de Serviços de Transporte, Empresas Terceirizadas ou Poder Concedente.
PERÍODO DE ARMAZENAMENTO DOS DADOS	O período de armazenamento deve seguir o princípio da minimização. Ou seja, os dados biométricos devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são tratados. Ainda que a LGPD não estabeleça um prazo limite para armazenamento dos dados biométricos, tão logo eles não sejam mais necessários ou adequados à finalidade da coleta, devem ser prontamente eliminados.

3.2.3. TRATAMENTO DE DADOS BIOMÉTRICOS DE COLABORADORES PARA FINS DE REGISTRO DE PONTO E CONTROLE DE JORNADA DE TRABALHO

TITULAR DOS DADOS	Colaboradores das prestadoras de serviços de transporte
FINALIDADE DO TRATAMENTO	Registro biométrico de ponto dos colaboradores. Ou seja, anotação do horário de entrada e saída dos colaboradores, a fim de contabilizar a jornada de trabalho.
POSSÍVEL BASE LEGAL	Art. 11, II, "a", da LGPD. Cumprimento de obrigação legal ou regulatória pelo controlador. O art. 74 da Consolidação das Leis do Trabalho (CLT) estipula a necessidade de registro de ponto (anotação do horário de entrada e saída do trabalho dos empregados), admitindo que ele se dê por meio manual, mecânico ou eletrônico. A Portaria nº. 1.510/2009 do Ministério do Trabalho autoriza o registro de ponto biométrico dos empregados.
AGENTES DE TRATAMENTO	Controlador: Prestadoras de Serviços de Transporte. Operador: Prestadoras de Serviços de Transporte e Empresas Terceirizadas.
PERÍODO DE ARMAZENAMENTO DOS DADOS	O período de armazenamento deve seguir o princípio da minimização. Ou seja, os dados biométricos devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são tratados. Ainda que a LGPD não estabeleça um prazo limite para armazenamento dos dados biométricos, tão logo eles não sejam mais necessários ou adequados à finalidade da coleta, devem ser prontamente eliminados.

3.2.4. TRATAMENTO DE DADOS BIOMÉTRICOS DE COLABORADORES PARA FINS DE CONTROLE DE ACESSO E SEGURANÇA

TITULAR DOS DADOS	Colaboradores das prestadoras de serviços de transporte
FINALIDADE DO TRATAMENTO	Permitir o acesso a determinados ambientes a pessoas expressamente autorizadas.
POSSÍVEL BASE LEGAL	Art. 11, II, "g", da LGPD. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto nos casos que prevalecem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
AGENTES DE TRATAMENTO	Controlador: Prestadoras de Serviços de Transporte. Operador: Prestadoras de Serviços de Transporte e Empresas Terceirizadas.
PERÍODO DE ARMAZENAMENTO DOS DADOS	O período de armazenamento deve seguir o princípio da minimização. Ou seja, os dados biométricos devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são tratados. Ainda que a LGPD não estabeleça um prazo limite para armazenamento dos dados biométricos, tão logo eles não sejam mais necessários ou adequados à finalidade da coleta, devem ser prontamente eliminados. Caso, por exemplo, seja retirado o direito de acesso a áreas restritas de determinado colaborador, os dados biométricos que eram utilizados para tal finalidade devem ser prontamente eliminados, ainda que o colaborador continue exercendo outras atividades dentro da empresa ou organização.

3.2.5. BOAS PRÁTICAS PARA O TRATAMENTO DE DADOS BIOMÉTRICOS NO SETOR DE TRANSPORTES

I. Para realizar a coleta de dados biométricos para fins de controle de acesso, as empresas e organizações devem demonstrar a necessidade de seu tratamento, indicando as razões concretas para o seu uso em detrimento de outros sistemas de identificação que não façam uso de dados biométricos, como a utilização de senhas ou de medidas organizacionais de segurança. A justificativa para o tratamento de tais dados pela empresa ou organização deve detalhar o contexto específico que torna necessário o alto nível de proteção conferido pela utilização de dados biométricos. Recomenda-se que a coleta de dados biométricos se restrinja, sempre que possível, ao controle de acesso a instalações da empresa ou organização que esteja sujeita à restrição de tráfego e a dispositivos e aplicativos de computação considerados de acesso restrito.

II. Recomenda-se que, para cada atividade/operação de tratamento de dados biométricos, independentemente da finalidade, as empresas e organizações elaborem um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), ou seja, uma avaliação do impacto sobre a proteção de dados, a fim de avaliar possível risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deve ser considerada especialmente para casos de tratamento de grande escala, ou seja, que visem uma grande quantidade de dados pessoais que possam afetar um número considerável de titulares de dados, e deve incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância das disposições da LGPD.

III. As empresas e organizações devem evitar o uso de autenticação biométrica fundada em amostragem biológica, como a coleta de saliva e sangue. Somado a isso, em todo e qualquer tratamento de dados biométricos, independentemente

da finalidade, é de responsabilidade das empresas e organizações justificar o tipo de método biométrico escolhido, seja a verificação da íris, impressão digital (palma da mão ou digital dos dedos), rede venosa da mão, formato da face, entre outros, em detrimento de outros menos invasivos. Por exemplo, especificamente para a finalidade de controle de acesso, antes de coletar os dados biométricos, as empresa e organizações devem sempre questionar (i) se a informação a qual se deseja proteger com a restrição do acesso realmente demanda a coleta de dado biométrico e (ii) se o nível de proteção o qual se busca conferir com o controle de acesso não pode ser assegurado de forma diversa, a partir da coleta tão somente de dados pessoais, mas não de dados pessoais sensíveis.

IV. Os documentos que amparam as políticas internas e externas de privacidade e tratamento de dados pessoais das empresas e organizações devem prever expressamente os motivos da coleta dos dados biométricos, a finalidade do seu tratamento, as medidas de segurança adicionais adotadas para a sua proteção e, inclusive, as hipóteses de término do tratamento e apagamento dos dados. Por exemplo, caso seja retirado o direito de acesso a áreas restritas de determinado colaborador, os dados biométricos que eram utilizados para tal finalidade devem ser prontamente eliminados, ainda que o colaborador continue exercendo outras atividades dentro da empresa ou organização. Nesse aspecto, recomenda-se ainda que, sempre que possível, as empresas e organizações adotem mecanismos adicionais de transparência quanto ao tratamento dos dados biométricos, a exemplo de uma aba de FAQ no site voltado para esse tema específico.

V. Sempre que o tratamento de dados biométricos for condição para o fornecimento de determinado serviço de transporte – a exemplo da recarga na bilhetagem eletrônica – o titular dos dados deverá ser informado, com destaque, em ambiente de fácil acesso e por meio de linguagem clara e simples, sobre esse fato e também sobre os meios pelos quais poderá exercer os direitos elencados no art. 18 da LGPD.

VI. **É fundamental que as empresas e organizações adotem medidas especiais para proteção desses dados, a exemplo da criptografia e do controle de acesso físico e lógico às bases de dados. Além disso, o tratamento de dados biométricos, independentemente da finalidade, deve ser minimamente ponderado à luz dos princípios da necessidade, adequação e finalidade, considerando a sensibilidade de tais dados, o volume necessário para realizar o tratamento e o fato de que, em caso de incidentes de segurança, o potencial dado eventualmente causado aos titulares é bastante considerável.**

3.3. PROTOCOLO DE EXAMES TOXICOLÓGICOS E TESTES DE BAFÔMETRO

Quanto ao exame toxicológico de largo espectro de detecção realizado em motoristas profissionais empregados (ou celetistas), destaca-se que é um exame capaz de detectar o consumo de substâncias psicoativas (drogas) em um período de tempo mais longo que os exames tradicionais de urina e sangue. Ele é capaz de detectar o uso de substâncias psicoativas (como maconha, crack, heroína, ecstasy, metanfetaminas, rebite, cocaína, entre outros) consumidas num período de 90 a 180 dias, dependendo do tipo de coleta (cabelos ou pêlos das pernas, braços, peito, axilas e pubianos), por meio da análise da queratina.

As categorias de motoristas profissionais que devem realizar o exame toxicológico periodicamente, conforme determinado por Lei, são: (i) motorista de furgão ou veículo similar; (ii) condutor de ambulância; (iii) motorista de ônibus rodoviário; (iv) motorista de ônibus urbano; (v) motorista de trólebus; (vi) caminhoneiro autônomo (rotas regionais e internacionais); (vii) motorista de caminhão (rotas regionais e internacionais) e (viii) motorista operacional de guincho, ou seja, todos motoristas profissionais que possuam Carteira Nacional de Habilitação (CNH) nas categorias C, D ou E.

Já o teste etilômetro (ou teste do bafômetro) é um meio de controle e fiscalização que pode ser feito pelas empresas prestadoras de serviços de transporte para

integrar o programa de controle de uso de drogas e bebida alcoólica previsto no art. 235-B da CLT. Para a implantação do teste, a empresa deve criar um regulamento específico contendo todas as informações referentes aos procedimentos que serão adotados, como os empregados serão submetidos ao exame, periodicidade, local para realização do exame, possibilidade de contraprova e as medidas que serão tomadas em caso de resultado positivo. Todos os empregados envolvidos deverão ter ampla ciência dos procedimentos, tendo em vista que a recusa em realizar o teste configura infração disciplinar, nos termos do art. 235-B, parágrafo único.

O critério de escolha para submissão ao exame deve ser objetivo – por exemplo, todos os empregados que exercem um tipo de função específica – para que se evite a discriminação. Com relação ao resultado do teste, diante da ausência de regulamentação própria e utilizando, por analogia, o dispositivo legal relativo ao exame médico toxicológico (art. 168 da CLT), este deve ser confidencial.

Os resultados do exame toxicológico e do teste de bafômetro enquadram-se na categoria de dados pessoais sensíveis, já que representam dados referentes à saúde dos motoristas profissionais, conforme prevê o 5º, inc. II,[1] da LGPD – o que implica na necessidade de que seu tratamento esteja amparado em uma das bases legais dispostas no art. 11.

3.3.1. OPERAÇÃO DE TRATAMENTO DE DADOS EM EXAMES TOXICOLÓGICOS E TESTES DE BAFÔMETRO

As atividades de tratamento de dados pessoais sensíveis em exames toxicológicos e testes de bafômetro realizadas pelas empresas e organizações do setor de transporte encontram-se relacionadas abaixo, com destaque às principais características do tratamento, que devem ser observadas por todos os destinatários do presente Guia de Boas Práticas.

1. Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

3.3.2. TRATAMENTO DE DADOS PESSOAIS DE MOTORISTAS PROFISSIONAIS CELETISTAS (OU EMPREGADOS) EM EXAMES TOXICOLÓGICOS DE LARGA JANELA DE DETECÇÃO

TITULAR DOS DADOS	Motoristas profissionais dos veículos de transporte.
FINALIDADE DO TRATAMENTO	Verificar o consumo de substancias psicoativas – sejam elas lícitas ou ilícitas – pelo motorista profissional contratado sob o regime celetista.
POSSÍVEL BASE LEGAL	AArt. 11, II, "a", da LGPD. Cumprimento de obrigação legal ou regulatória pelo controlador. Os arts. 168, §§ 8º e 9º, e 235-B, VII, da CLT estipulam a exigência de realização de exames toxicológicos com janela de detecção mínima de 90 (noventa) dias por motoristas profissionais celetistas para substâncias psicoativas que causem dependência ou comprometam a capacidade de direção. Além disso, a Portaria nº. 116/2015 do Ministério do Trabalho e Previdência Social regulamenta a realização dos exames toxicológicos previstos nos §§ 6º e 7º do art. 168 da CLT. Por fim, o Código de Trânsito Brasileiro (CTB) normatiza em seu art. 165-A penalidade de multa por se recusar a soprar o bafômetro.
AGENTES DE TRATAMENTO	Controlador: Prestadoras de Serviços de Transporte e Ministério da Economia (co-controladores). O art. 2º da Portaria nº. 945/2017 do Ministério do Trabalho exige, das empresas contratantes de motoristas profissionais CLT, a inserção dos dados do resultado do exame toxicológico no eSocial sempre que este for admitido ou desligado. Os resultados detalhados dos exames devem ficar armazenados em formato eletrônico pelo laboratório executor por no mínimo 5 (cinco) anos.

Protocolos Específicos

3.3.3. TRATAMENTO DE DADOS PESSOAIS DE MOTORISTAS PROFISSIONAIS CELETISTAS (OU EMPREGADOS) EM TESTES DO ETILÔMETRO (OU TESTE DE BAFÔMETRO)

TITULAR DOS DADOS	Motoristas profissionais dos veículos de transporte.
FINALIDADE DO TRATAMENTO	Verificar o consumo de álcool no sangue do motorista profissional contratado sob o regime celetista.
POSSÍVEL BASE LEGAL	Art. 11, II, "a", da LGPD. Cumprimento de obrigação legal ou regulatória pelo controlador. O art. 235-B, VII, da CLT estipula a obrigação de que o motorista profissional empregado (ou celetista) submeta-se ao programa de controle de uso de droga e de bebida alcoólica instituído pela empresa prestadora de serviços de transportes para a qual trabalha, desde que prévia e amplamente cientificado.

3.3.4. BOAS PRÁTICAS NO TRATAMENTO DE DADOS EM EXAMES TOXICOLÓGICOS E TESTES DE BAFÔMETRO

I. **Durante a realização do teste de bafômetro, é fundamental que a privacidade do motorista seja resguardada, tendo em vista que as informações coletadas dizem respeito a aspectos da sua intimidade cuja eventual exposição pode lhe causar dano, especialmente quando o resultado do teste for positivo e atestar a presença de álcool no sangue. As empresas e organizações devem também garantir a confidencialidade dos resultados dos exames toxicológicos e testes de bafômetro, especialmente em caso de resultado positivo. Para zelar pela confidencialidade do exame, e de seu resultado, o teste deve ser feito em local reservado, sem interferência ou possibilidade de acompanhamento por outras pessoas, de maneira que o motorista que será testado não seja exposto.**

Protocolos Específicos

II. Os dados pessoais coletados no etilômetro para fins de aferição da presença de álcool no sangue do motorista não podem ser utilizados para outra finalidade que não seja compatível com esta. Nesse sentido, recomenda-se que tais dados não sejam tratados para fins de controle de pontualidade ou controle de jornada sem o conhecimento dos motoristas. Isso porque, nesse caso, além de a nova finalidade (controlar se os motoristas chegam atrasados no trabalho) não estar relacionada com a original (controlar a presença de álcool no sangue), há que se destacar ainda outros fatores, como o potencial impacto negativo sobre o empregado – que poderá sofrer um procedimento disciplinar interno, inclusive com punições ou possível demissão –, a natureza sensível dos dados, a obrigação legal do motorista de fornecer tais informações e o desequilíbrio de poder entre o motorista e a empresa prestadora dos serviços de transporte.

III. Os dados referentes aos resultados dos exames toxicológicos de motoristas profissionais celetistas – mesmo que não tenham sido contratados ou que já tenham sido demitidos – devem ser armazenados em ambiente separado dos demais dados e ter seu acesso restrito a pessoas expressamente autorizadas e que realmente necessitem acessá-los para exercer sua função dentro da empresa.

IV. O tratamento dos dados relacionados ao resultado do teste de bafômetro deve ser realizado conforme o princípio da não discriminação, previsto no art. 6º, IX, da LGPD. Exatamente por isso, todo o procedimento deve ser realizado seguindo os critérios da objetividade, não discriminação, e deverá ser documentada cada etapa, bem como, diante da necessidade, será necessário o acompanhamento e assinatura de testemunhas.

V. As empresas e organizações devem documentar e divulgar amplamente para os motoristas profissionais empregados (ou celetistas) as informações relacionadas ao tratamento de dados pessoais sensíveis resultantes dos exames toxicológicos e testes de bafômetro, incluindo forma de armazenamento, tempo de retenção, finalidade do tratamento, entre outros.

Anexos

ANEXO I

MARCO NORMATIVO E LEGISLAÇÃO SETORIAL DE PROTEÇÃO DE DADOS NO SETOR DE TRANSPORTES

LEIS E DECRETOS

• **Lei nº. 11.442**, de 5 de janeiro de 2007, que dispõe sobre o transporte rodoviário de cargas por conta de terceiros e mediante remuneração.

• **Lei nº. 13.103,** de 2 de março de 2015, que dispõe sobre o exercício da profissão de motorista e disciplina a jornada de trabalho e o tempo de direção do motorista profissional.

• **Lei nº. 9.506,** de 23 de setembro de 1997, que institui o Código de Trânsito Brasileiro.

• **Decreto-Lei nº. 5.452,** de 1º de maio de 1943, que aprova a Consolidação das Leis do Trabalho.

• **Lei nº. 14.071,** de 13 de outubro de 2020, que modifica a composição do Conselho Nacional de Trânsito e amplia o prazo de validade das habilitações.

• **Decreto nº. 8.033,** de 27 de junho de 2013, que regulamenta as disposições legais que regulam a exploração de portos organizados e de instalações portuárias.

• **Decreto nº. 8.071,** de 14 de agosto de 2013, que regulamenta as disposições legais que regulam a exploração de portos organizados e de instalações portuárias.

• **Lei nº. 14.047,** de 24 de agosto de 2020, que dispõe sobre medidas temporárias para enfrentamento da pandemia da Covid-19 no âmbito do setor portuário, sobre a cessão de pátios da administração pública e sobre o custeio das despesas com serviços de estacionamento para a permanência de aeronaves de empresas nacionais de transporte aéreo regular de passageiros em pátios da Empresa Brasileira de Infraestrutura Aeroportuária (Infraero).

Anexos

• **Decreto nº. 6.759,** de 5 de fevereiro de 2009, que regulamenta a administração das atividades aduaneiras, e a fiscalização, o controle e a tributação das operações de comércio exterior.

• **Decreto nº. 7.373,** de 11 de dezembro de 2014, que institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (e-Social).

• **Lei nº. 8.213,** de 24 de julho de 1991, que dispõe sobre os Planos de Benefícios da Previdência Social.

• **Lei nº. 10.097,** de 19 de dezembro de 2000, que altera dispositivos da Consolidação das Leis do Trabalho (CLT).

• **Lei nº. 9.611,** de 19 de fevereiro de 1998, que dispõe sobre o Transporte Multimodal de Cargas e dá outras providências.

• **Lei nº 12.587,** de 3 de janeiro de 2012, que institui as diretrizes da Política Nacional de Mobilidade Urbana.

• **Lei nº 8.987,** de 13 de fevereiro de 1995, que dispõe sobre o regime de concessão e permissão de serviços públicos.

• **Lei nº 14.133,** de 1 de abril de 2021, que estabelece normas gerais de licitação e contratação.

RESOLUÇÕES NORMATIVAS DA AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS (ANTAQ)

• **Resolução nº. 517,** de 18 de outubro de 2005, que aprova a norma para outorga de autorização para a construção, a exploração e a ampliação de terminal portuário de uso privativo.

• **Resolução nº. 3.220,** de 9 de janeiro de 2014, que aprova a norma que estabelece procedimentos para a elaboração de projetos de arrendamentos e recomposição do equilíbrio econômico-financeiro dos contratos de arrendamento de áreas e instalações portuárias nos portos organizados.

Anexos

• **Resolução Normativa nº. 7,** de 2 de junho de 2016, que aprova a norma que regula a exploração de áreas e instalações portuárias sob gestão da administração do porto, no âmbito dos portos organizados.

• **Resolução nº. 7.821,** de 22 de junho de 2020, que dispõe sobre os procedimentos para elaboração da versão simplificada dos estudos prévios mencionados no art. 6º, § 1º, inciso IV do Decreto nº 8.033, de 2013.

• **Resolução nº. 3.106,** de 16 de outubro de 2013, que aprova o modelo de formulário para requerimento de adesão ao regime especial de incentivos para o desenvolvimento da infraestrutura (REIDI).

• **Resolução Normativa nº. 20,** de 16 de maio de 2018, que aprova a proposta de norma que dispõe sobre a autorização para a construção e exploração de terminal de uso privado, de estação de transbordo de carga, de instalação portuária pública de pequeno Porte e de instalação portuária de turismo.

RESOLUÇÕES NORMATIVAS DA AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES (ANTT)

• **Resolução nº. 4.799,** de 27 de junho de 2015, que regulamenta procedimentos para inscrição e manutenção no Registro Nacional de Transportadores Rodoviários de Cargas (RNTRC).

• **Resolução nº. 5.840,** de 22 de janeiro de 2019, que dispõe sobre o transporte rodoviário internacional de cargas.

• **Resolução nº. 5.879,** de 26 de março de 2020, que dispõe sobre a flexibilização de prazos para cumprimento de obrigações contratuais e regulatórias, em razão da emergência de saúde pública de importância internacional decorrente do coronavírus, no âmbito da infraestrutura e serviço de transporte ferroviário de cargas e do transporte rodoviário de cargas e de passageiros.

• **Resolução nº. 5.396,** de 3 de agosto de 2017, que regulamenta a oferta de tarifa promocional para os serviços de transporte rodoviário e ferroviário regular interestadual e internacional de passageiros e semiurbano de passageiros.

Anexos

• **Resolução nº. 5.063,** de 30 de março de 2016, que dispõe sobre procedimentos a serem observados na aplicação do Estatuto da Juventude no âmbito dos serviços de transporte rodoviário e ferroviário interestadual de passageiros, e dá outras providências.

• **Resolução nº. 4308,** de 10 de abril de 2014, que dispõe sobre a sistemática de identificação dos passageiros dos serviços de transporte rodoviário e ferroviário de passageiros regulados pela ANTT.

• **Resolução nº. 4.282,** de 17 de fevereiro de 2014, que dispõe sobre as condições gerais relativas à venda de bilhetes de passagem nos serviços regulares de transporte terrestre interestadual e internacional de passageiros regulados pela ANTT.

• **Resolução nº. 3.535,** de 10 de junho de 2010, que fixa normas gerais sobre o Serviço de Atendimento ao Consumidor (SAC) nos serviços de transporte rodoviário interestadual e internacional de passageiros, de transporte ferroviário de passageiros ao longo do Sistema Nacional de Viação e de exploração da infraestrutura das rodovias concedidas e administradas pela ANTT.

• **Resolução nº. 2.030,** de 23 de maio de 2007, que dispõe sobre procedimentos a serem observados na aplicação do Estatuto do Idoso, no âmbito dos serviços de transporte ferroviário interestadual regular de passageiros.

• **Resolução nº. 1.603,** de 29 de agosto de 2006, que estabelece critérios e procedimentos para o acompanhamento do treinamento do pessoal operacional e administrativo, próprio ou de terceiros, das concessionárias de serviço público de transporte ferroviário de cargas e de passageiros.

OUTRAS NORMATIVAS

• **Circular nº. 422,** de 1º de abril de 2011, da SUSEP, que estabelece as regras básicas para a comercialização do Seguro de Responsabilidade Civil do Transportador Rodoviário por Desaparecimento de Carga (RCF-DC), e disponibiliza, no endereço eletrônico da SUSEP, as condições contratuais do Plano Padronizado deste seguro.

Anexos

• **Portaria n. 6.734,** de 9 de março de 2020, do Ministério da Economia, que aprova a nova redação da Norma Regulamentadora nº 07 – Programa de Controle Médico de Saúde Ocupacional – PCMSO.

• **Portaria nº. 131,** de 4 de maio de 2010, da Secretaria dos Portos (SEP), que estabelece procedimentos para registro, elaboração e seleção de projeto básico de Empreendimentos Portuários marítimos passíveis de concessão.

• **Resolução nº. 47,** de 7 de abril de 2011, da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS), que dispõe sobre critérios para a realização de auditorias nas instalações portuárias, em conformidade com o Código Internacional de Proteção de Navios e Instalações Portuárias - ISPS Code, e dá outras providências.

• **Portaria nº. 124,** de 30 de agosto de 2013, da Secretaria dos Portos (SEP), que estabelece os procedimentos para aprovação dos projetos de investimento em infraestrutura portuária tendo em vista o Regime Especial de Incentivos para o Desenvolvimento da Infraestrutura (REIDI).

• **Portaria nº. 512,** de 27 de setembro de 2018, do Ministério dos Transportes, Portos e Aviação Civil, que disciplina procedimentos e requisitos de aprovação de enquadramento de projetos para implantação de obras de infraestrutura de transportes, para fins de habilitação ao Regime Especial de Incentivos para o Desenvolvimento da Infraestrutura (REIDI).

• **Portaria nº. 111,** de 7 de agosto de 2013, da Secretaria dos Portos (SEP), que estabelece as normas, os critérios e os procedimentos para a pré-qualificação dos operadores portuários de que trata o inciso IV do art. 16 da Lei nº 12.815, de 5 de junho de 2013.

• **Resolução nº. 52,** de 27 de dezembro de 2018, da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS), que dispõe acerca da consolidação e atualização das Resoluções da CONPORTOS, conforme normas do Código Internacional para a Proteção de Navios e Instalações Portuárias – Código ISPS.

Anexos

• **Portaria nº. 3.518,** de 3 de outubro de 2011, da Receita Federal do Brasil, que estabelece requisitos e procedimentos para o alfandegamento de locais e recintos.

• **Ato Declaratório Executivo nº. 2,** de 1º de novembro de 2003, da Receita Federal do Brasil, que especifica os requisitos técnicos, formais e prazos para implantação de sistema informatizado de controle aduaneiro domiciliar e de recintos alfandegários ou autorizados a operar com mercadorias sob controle aduaneiro.

• **Resolução 326,** de 10 de junho de 2014, da Agência Nacional de Aviação Civil. RPAC 120/ANAC - Regulamento Brasileiro da Aviação Civil - Programa de prevenção do risco associado ao uso indevido de substâncias psicoativas na aviação civil.

Anexos

ANEXO II
ELEMENTOS DE CONFORMIDADE DE FEDERAÇÕES E SINDICATOS DO SETOR DE TRANSPORTE À LGPD

As relações *business-to-business* (B2B), ou seja, entre pessoas jurídicas, diferem das relações *business-to-costumer* (B2C), que são realizadas entre empresas do setor de transporte e passageiros, ou mesmo entre empresa do setor de transporte e o consumidor final em caso de e-commerce, em diversos aspectos, a exemplo da finalidade de coleta. No entanto, é certo que ambas apresentam suas próprias complexidades.

Como se sabe, as entidades representativas (Confederação, federações, sindicatos e associações) do setor de transportes também tratam dados pessoais em sua atividade, sejam dados de seus afiliados quando pessoas naturais ou empregados, seja de eventuais parceiros, prestadores de serviço e demais terceiros. Em geral, os dados pessoais tratados por essas entidades têm a finalidade de atender às exigências do contrato de trabalho, legislação previdenciária e trabalhista para empregados diretos, além de execução dos contratos e, por vezes, cumprimento de obrigações legais ou regulatórias.

Nota-se, nesse sentido, que as bases legais mais comuns de tratamento dos dados nessas hipóteses mencionadas costumam ser (i) o cumprimento de obrigação legal ou regulatória pelo controlador; e (ii) a necessidade dos dados para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular dos dados a seu pedido. Assim, destacam-se a seguir algumas diretrizes específicas de conformidade à LGPD aplicáveis às entidades representativas do setor de transporte, sem prejuízo da observação por estas entidades dos elementos gerais trazidos no presente Guia.

Anexos

DIRETRIZES SOBRE O CICLO DE VIDA DOS DADOS

As diretrizes internas das entidades representativas e os seus fluxos de dados devem prever regras claras sobre o tratamento de dados de seus empregados e filiados, a fim de priorizar a sua tutela em todos os processos a serem executados. Cabe lembrar que essas normas deverão prever regras sobre, entre outros aspectos, coleta, armazenamento, compartilhamento e descarte das informações, respeitando as diretrizes da LGPD. Dessa forma, sugere-se um conjunto mínimo de medidas de conformidade:

Mapeamento. Elaborar uma pesquisa inicial e mapear o fluxo de dados nos processos de tratamento de dados pessoais realizados pelas entidades representativas. A partir do montante dos dados pessoais levantados, deve-se visualizar os fluxos e processos e categorizar os riscos que envolvem dados pessoais, com o fim de definir as ações de gestão e resposta. A partir desse levantamento, será possível localizar onde as informações estão armazenadas, quem as acessa e por onde e com quem são compartilhadas, auxiliando no enquadramento das hipóteses legais autorizativas de tratamentos.

Avaliação de riscos e implementação. A partir do mapeamento, deve ser realizada uma análise objetivando verificar os procedimentos necessários e processos a serem iniciados para que os tratamentos de dados se adequem às diretrizes da LGPD. Também é necessária a revisão e atualização das cláusulas de contratos de que as entidades representativas são parte para atualizar os parâmetros relacionados à proteção de dados e mitigar riscos inerentes à terceirização de processamento de dados e compartilhamento com terceiros.

Anexos

Educação e sensibilização. Sugere-se, às entidades representativas, a elaboração de documentos de natureza orientativa acerca de práticas de proteção de dados, bem como de documentos dirigidos a profissionais conforme funções e necessidades específicas, como guias sobre procedimentos de segurança da informação.

Descarte. Deve-se assegurar, através de um procedimento interno da equipe de TI, em conformidade com a LGPD, que os dados sejam descartados quando findar a necessidade de tratamento, quando este for realizado para cumprimento de obrigação legal ou regulatória.

DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

As entidades representativas devem, preferivelmente, implementar um comitê de crise corporativo formado por áreas multidisciplinares para tratar da gestão de incidentes de dados pessoais. Tanto o ambiente digital quanto o físico, no que tange aos bancos de dados, devem ser monitorados quanto a acessos indevidos ou tentativas, externos e internos. Deve-se também garantir o funcionamento dos sistemas de logs dos servidores, como forma de garantir a rastreabilidade de acessos, além da implementação dos recursos técnicos de segurança da informação aptos a garantir os dados pessoais na medida de sua natureza e do risco que um incidente possa representar aos seus titulares.

As entidades representativas devem ter conhecimento de quem controla ou tem acesso a informações pessoais, sejam de seus funcionários ou filiados ou de eventuais parceiros, prestadores de serviço e terceiros no geral. Devem ser realizados testes periódicos de segurança para os bancos de dados e realizados treinamentos para os funcionários que tenham acesso a informações confidenciais, reservadas ou privilegiadas.

Anexos

DIRETRIZES PARA COMPARTILHAMENTO DE DADOS

Como parte relevante dos dados pessoais compartilhados são relativos aos casos de atendimento às obrigações legais, como eSocial, DIRF – Imposto de Renda, RAIS – Informações Sociais, comunicação de acidente de trabalho (previdência social) e pagamentos de FGTS, pagamentos de benefícios e seguradoras, é fundamental que as entidades representativas somente compartilhem dados coletados de seus membros com o devido suporte na respectiva base legal. O compartilhamento deve estar assegurado a partir do próprio contrato de trabalho, através de cláusula própria.

Quando houver o compartilhamento de dados biométricos para fins de registro e apuração do ponto, caso o sistema de processamento desses dados seja terceirizado e apenas a coleta seja de responsabilidade das entidades representativas, deve-se especificar no contrato com a empresa terceirizada as competências pela gestão e responsabilização dos dados e assegurar-se de que a empresa possa fornecer a devida garantia de cumprimento das obrigações decorrentes da LGPD.

CNT | SEST SENAT | ITL

Setor de Autarquias Sul / Quadra 1 / Bloco J
Edifício Clésio Andrade / 14º andar
CEP 700070-944 / Brasília / DF

Central de Relacionamento
0800 728 289 / www.cnt.org.br